DICIEMBRE 2023

ASOCIACIÓN DE INGENIEROS DEL URUGUAY

Ingeniería

N°98



Hidrógeno

Ing. Gustavo Mesorio

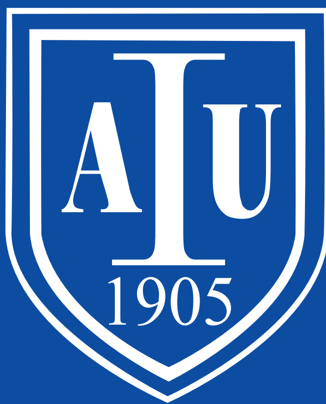
Generalidades sobre sistemas de sonido domésticos

Ing. Javier Beltrame

Análisis de seguridad de una arquitectura referencial de la plataforma FIWARE

Ing. Juan Pablo Perata
Ing. Gustavo Betarte





Asociación de Ingenieros del Uruguay

Acompañando a la Ingeniería desde 1905

REDACTOR RESPONSABLE
Mag. Ing. Miguel Fierro

DISEÑO EDITORIAL
www.disenio.net

IMPRESIÓN Y ENCUADERNACIÓN
Gráfica Mosca
Nº de depósito 358055

Contenido


AIU
1905



Asociación de Ingenieros del Uruguay

Acompañando a la Ingeniería desde 1905

¿Qué es AIU?

La AIU es una asociación civil con finalidad gremial fundada el 12 de octubre de 1905, con personería jurídica reconocida por Resolución del Poder Ejecutivo de fecha 28 de julio de 1922.

¿Qué buscamos?

Ser reconocidos como una institución referente de la ingeniería nacional y contribuir mediante su superación al desarrollo de la ingeniería del país, al progreso y bienestar social y a la dignificación personal.

¿Qué hacemos como asociación?

Fortalecemos permanentemente la institución para beneficio de sus asociados, de la profesión en general y de la sociedad. Promovemos la comunicación y el intercambio técnico y de experiencias entre asociados. Nos relacionamos con instituciones nacionales y extranjeras.



Asociate

Participá de los eventos
y actividades que tenemos
para ofrecerte

Asociación de Ingenieros del Uruguay

Cuareim 1492
(+598) 2901 1762 / 2900 8951
(+598) 98 869 645
aiu@vera.com.uy
www.aiu.org.uy

aingenierosu
aingenierosu
aingenierosu
@aingenierosu
Asociación de Ingenieros del Uruguay

Asamblea General FMOI

Autor
Mag. Ing. Miguel Fierro



El 14 de octubre de 2023 se llevó a cabo en la ciudad de Praga, República Checa la Asamblea General de la Federación Mundial de Organizaciones de Ingeniería.

En la misma se hicieron presentes delegaciones de 76 países miembros en modalidad híbrida. (presencial y por zoom). Se emitieron mensajes grabados del Secretario General de Naciones Unidas Antonio Guterres y de la asistente del director general de UNESCO, Lidia Brito.

En la reunión del foro de jóvenes ingenieros que tuvo lugar el 11 de octubre, la Past President de FMOI, Marlene Kanga hizo el lanzamiento de la Hackaton que se estará celebrando el 4 de marzo de 2024, día mundial de la ingeniería.

El día 13 de octubre se realizó la reunión del comité ejecutivo de FMOI durante el cual se aprobaron una serie de reglamentos y procedimientos de la Federación, para efectivizar y transparentar los procesos de decisión y electorales. También se aprobó la actualización del código de ética y la aceptación de nuevas instituciones miembros, los Ingenieros de Irlanda como miembros nacionales, la Academia de Ingeniería de Azerbaiyán como miembro nacional, El American Board of Engineering and Technology (ABET), USA, como miembro afiliado, la IEEE como miembro asociado y la Royal Academy of Engineering, UK, como miembro asociado. Finalmente se aprobaron los premios a la mujer en la ingeniería, la excelencia en la ingeniería en construcción y la excelencia en la ingeniería en educación.

En esta instancia hubo también elecciones de presidente, vicepresidente y miembros del consejo ejecutivo. El presidente electo resultó ser el Sr. Seng Chuan Tan del Instituto de Ingenieros de Singapur para el periodo 2025-2027, para el cargo de vicepresidente ejecutivo fue electa la Sra. Ania Lopez del Consejo Nacional de Ingenieros de Italia para el periodo 2023-2027 y como representantes miembros nacionales la Sra. Nahla Ahmed Al Qasimi de la Sociedad de Ingenieros de Emiratos Árabes, la Sra. He Jing de la Asociación de Ciencia y Tecnología de China, el Sr. Nathaniel Matalanga del Instituto de Ingenieros de Kenya, el Sr. Navichandra Vasoya del Instituto de Ingenieros de India y el Mag. Ing. Miguel Fierro de la Asociación de Ingenieros del Uruguay.

Fueron renovados los cargos de presidentes de los distintos comités técnicos, se destacan los cambios en el Comité de Energía que será liderado por la Sra. Marie-Line Vaiani del Ingenieros y Científicos de Francia y la designación como vicepresidente para América Latina del Mag. Ing. Miguel Fierro.

Se definió por votación la designación de la sede de la asamblea anual en 2025 a la ciudad de Shanghái propuesta por la Asociación de Ciencia y Tecnología de China.

Se firmó un Memorándum de entendimiento entre la FMOI y Ingenieros sin Fronteras, Engineers Whithout Borders (EWB).

Finalizada la Asamblea General el presidente José Vieira formalmente traspasó el mando al presidente electo Mustafa Shelu para el periodo 2023-2024.

A continuación se transcribe la declaración de Praga:



The Prague Declaration

The 7th World Engineers Congress organised by the Czech Association of Scientific and Technical Societies (CSVTS) in collaboration with the World Federation of Engineering Organizations brought together leading engineers from around the world to address urgent planetary challenges and explore how technological innovations and transdisciplinary approaches can deliver environmental, social and economic sustainability to ensure a safe, fair, healthy and peaceful future.

Considering that:

- The UN´s Sustainable Development Goals provide the framework to address the unprecedented global challenges facing humanity which threaten our future well-being and quality of life;
- The engineering fraternity has a responsibility to contribute to addressing the Goals and finding solutions;
- Climate change is the most critical and urgent issue of our times;
- Strengthening links between education, science, engineering and policy is essential if we are to achieve the Goals by 2030;
- Covid-19, the UKraine war and energy have underlined the essentiality of resilience, security and risk awareness along with social concerns;
- There is an inextricable link between engineering and life which can make profoundly positive contributions to the world;
- Government, business and industry must work in partnership to accelerate positive change;
- Our natural resources are finite and biodiversity is facing major threats;
- We need innovative engineering, to advance the Circular Economy;
- Engineering is key to delivering the much-needed paradigm shift and Will require concerted efforts to increase the number of engineering graduates;

Accordingly the delegates of WEC 2023 declare that engineers will:

- Address agriculture and natural resources and develop solutions to maintain the balance between energy, water, food, soil fertility and deforestation;
- Develop solutions that mitigate the negative impacts of human activities on ecosystems and species;
- Ensure that computers, robots artificial intelligence and other technologies are used responsibly, ethically and safely, and do not cause harm;
- Take a more active role in addressing issues related to cybersecurity and privacy risks;
- Improve energy security by developing, implementing, and maintaining systems and technologies that ensure reliable and resilient energy supply;
- Develop innovative technologies necessary to ensure the reliability, safety and economy of emerging energy systems based on renewable energy sources;
- Improve energy storage technologies and develop Smart grids to enable efficient and flexible energy distribution;
- Develop and implement technologies, strategies, and solutions that reduce greenhouse gas emissions and address the causes of global warming;
- Support the education of engineers, their professional development and training to for new technologies in industrial and developing countries;
- Develop low-energy and low-emission industrial technologies and processes, ensuring low-material usage, recycling, waste management and supporting a circular economy;
- Develop technologies and solutions that create income-generating opportunities for marginalized communities;
- Design medical devices and healthcare technologies that improve diagnosis, treatment, and healthcare access, particulary in remote areas;
- Develop technologies and systems that empower women economically, socially, and educationally;
- Provide access to clean water and sanitation solutions;
- Develop accessible infrastructure for people with disabilities;

- Contribute to technology solutions for crime prevention, law enforcement, and justice systems;
- Design and construct efficient and eco-friendly transportation networks, such as public transport, cycling lanes, and pedestrian pathways and ensure the transition to electric, hybrid, and alternative fuel vehicles;
- Support sustainable city development by collaborating with urban planners to create mixed-use developments that reduce the need for long commutes, encouraging walking and cycling.

Engineers are masters in creativity, finding new ways to solve or work around problems while creating inventive fail-safes and minimising risks to maximise endurance, funcionality and efficiency.

It is fitting that the engineering profession delivers this important Declaration in the city of Prague where the world´s first engineering institution dedicated to education was established in 1707 by Christian Josef Willenberg, which laid the foundation for the development of engineering schools globally.

Signed
Prof. Daniel Hanus
President
CSVTS

Signed
Prof. Jose Vieira
President
World Federation of Engineering Organisations







Asamblea General UPADI

Autor
Mag. Ing. Miguel Fierro

El 14 de setiembre se llevó a cabo en la ciudad de Antigua, República de Guatemala la Reunión Ordinaria n° 566 de la Unión Panamericana de Asociaciones de Ingenieros.

En la misma se hicieron presentes 15 países miembros activos y tres miembros observadores en modalidad híbrida. (presencial y por zoom).

Se trataron temas administrativos, contables y organizativos. Todos los asistentes hicieron uso de la palabra presentando informes verbales sobre las actividades realizadas por sus respectivas asociaciones y colegios en este último año.

El día 13 de setiembre se realizó el Simposio Técnico organizado por el Consejo Técnico de UPADI con la participación destacada de 17 panelistas, cada uno de ellos experto en su campo de acción. Toda la actividad contó con la participación de profesionales tanto en forma presencial como virtual. Se discutió sobre el futuro del Comité de Energía y finalmente se definió que la sede sea en Uruguay, recomendándose que su presidente sea el Mag. Ing. Miguel Fierro.

El Ing. Olman Vargas, presidente del Colegio de Ingenieros Civiles de Costa Rica presentó el informe del Consejo Consultivo en nombre de su presidenta la Ing. Irene Campos. Se propuso la inclusión en el consejo consultivo del Ing. Edemar Amorin, se aprobó la moción y se validó en la asamblea.

El Tesorero, Mag. Ing. Miguel Fierro puso a consideración de la asamblea el balance del periodo octubre 2022-setiembre 2023 y el presupuesto 2024 los cuales fueron aprobados por unanimidad. En lo que respecta a las obligaciones ante FMOI se informó que estaban al día.

El presidente de UPADI, Ing. Aridai Herrera hizo un raconto de sus actividades en el periodo abril 2023-setiembre 2023 y presentó un reporte de infraestructura (PEER). Se leyó la carta de renuncia del ing. Jorge Spitalnik al cargo de Director Ejecutivo de UPADI y el presidente de la Academia Panamericana de Ingeniería ofreció para jóvenes ingenieros de hasta 10 países miembros de UPADI una semana de alojamiento y comida en Puerto Rico con visitas técnicas a distintas obras de ingeniería.

El Colegio de Ingenieros del Perú será el anfitrión de la asamblea anual en el año 2024, en Lima donde se festejarán los 75 años de la creación de UPADI.

A continuación, se transcribe la declaración de Antigua

Un Llamado a la Acción a los Líderes Mundiales para:

La Educación y Desarrollo de La Ingeniería.

La Mitigación de Daños por Desastres Naturales,

El Diseño y Construcción de Obras Resilientes y Acciones Afirmativas contra el Impacto del Cambio Climático

Reunidos en la ciudad de Antigua Guatemala, en el día de la celebración de La Declaración de Independencia de las Repúblicas de Costa Rica, Guatemala, Honduras, Nicaragua y El Salvador, los miembros de La Unión Panamericana de Asociaciones Ingeniería, UPADI, conscientes de la responsabilidad de los ingenieros con la "Educación y Desarrollo de la Ingeniería para Mitigar Daños por Desastres Naturales, Diseñar y Construir Obras Resilientes, y Paliar el Impacto del Cambio Climático" acuerdan reiterar, exponer y compartir sus conclusiones con los profesionales y las autoridades de todos los países del hemisferio y del mundo como se reseña; en ese sentido, se retoman declaraciones anteriores, que siguen siendo vigentes y necesarias al día de hoy, con el fin de insistir en la concientización de los profesionales de ingeniería en ser parte de la solución de tan significativos (problemas) retos. Una Prioridad Mundial A pesar de la amplia difusión de información y de los esfuerzos concertados en todo el planeta, las emisiones de gases de efecto invernadero no han logrado reducirse. Su impacto en el Cambio Climático incide sobre la frecuencia y magnitud de desastres naturales y sus consecuencias; la pérdida de vidas humanas, fauna y flora, la destrucción de ecosistemas y medios de subsistencia para la humanidad y la destrucción de viviendas, escuelas, hospitales e infraestructura. Este impacto se cierne con mayor intensidad sobre las más vulnerables poblaciones, las comunidades marginadas, las pequeñas islas y los países en vías de desarrollo. 10 Mitigar el Impacto de los Desastres Relacionados con el Clima Para lograr los objetivos de Desarrollo Sostenible trazados para el año 2030 y de Cero Emisiones netas para el año 2050, se estima necesario invertir anualmente en infraestructura que permitan un futuro de bajas emisiones de carbón y resiliente al clima. La inversión efectiva de tal cantidad de recursos requiere acciones concertadas de los responsables de la planificación, desarrollo, diseño, construcción y operación de cada obra. Siendo las emisiones de CO2, con otros factores, el resultado de actividades humanas como el desarrollo y la construcción corresponde a los responsables de la planificación, diseño, construcción y operación de toda clase obras, el integrar en todos los procesos, medidas para reducir, minimizar y mitigar las emisiones de carbono y adaptarse al cambio climático. La construcción sostenible y resistente a los embates del clima representa la ruta a seguir para lograr la Resiliencia, lograr el objetivo Cero Neto y asegurar el bienestar de todos los ecosistemas y la humanidad. El fracaso no es una opción y toca a los Ingenieros asumir la Responsabilidad El emprendimiento convencional de proyectos de infraestructura no ha logrado alcanzar los objetivos expuestos, y las consecuencias morales de fracasar son inaceptables. Es imprescindible el desarrollo y construcción de obras que permitan un futuro de bajas emisiones de carbón y resiliente al clima para paliar el impacto del cambio climático y garantizar la mejor calidad de vida para todos. Para lograr los objetivos del Acuerdo de París y de Desarrollo Sostenible es insoslayable incorporar a los ingenieros en la planificación de todos los proyectos desde su concepción hasta la operación, integrando conocimiento del comportamiento humano, gestión del conocimiento y manejo de medios y comunicaciones en la todas las fases de la gestión de proyectos. Este protagonismo requiere que se integren conocimientos gerenciales a la formación técnica de los ingenieros, para lo cual deben desarrollarse alianzas Universidad/Industria que permitan a los jóvenes ingenieros aportar su creatividad y espíritu emprendedor temprano en su desempeño profesional y así lograr obras sostenibles, resilientes que perduren. El Impacto del Cambio Climático en el Ordenamiento Jurídico 11 Resulta imperativo reconocer las consecuencias del impacto climático sobre la superficie de la tierra, costas, glaciares, océanos, mares, lagos, cuencas de ríos, mangles y humedales. Esta realidad incide ya sobre terrenos en costas y de riberas donde ya conflige el derecho a la propiedad privada con el derecho a la utilización de zonas de esparcimiento y la explotación del patrimonio común. En consecuencia, sin mayor dilación, debe atemperarse el ordenamiento jurídico para asegurar la resolución de conflictos que pueden vislumbrarse en cada país, así como en el ámbito internacional. . Para discurrir de las Palabras a la Acción se propone Concretamente: 1. Incorporar, primero y sobre todo, el conocimiento de los científicos, ingenieros y profesionales en las normas de diseño, códigos de construcción, modernización, construcción y operación de toda obra de pública y privada, así como en la gestión de riesgos inherentes a cada obra. 2. Difundir el impacto del Cambio Climático y de cómo se puede contribuir a minimizar el impacto a través de la educación pública desde los niveles primarios. 3. Proponer Códigos técnicos y criterios de desempeño que den a los profesionales en ingeniería las herramientas necesarias para solucionar los problemas generados por el Cambio Climático 4. Hay que asegurar que en toda toma de decisiones, se da especial consideración a las circunstancias de las poblaciones de los países y las comunidades más vulnerables 5. Integrar la construcción verde y soluciones cónsonas con la naturaleza en todo desarrollo 6. Promover e implementar financiamiento justo, inclusivo y sostenible en toda construcción 7. Reforzar la infraestructura esencial para lograr su resiliencia al cambio climático 8. Mitigar la vulnerabilidad de toda obra a los desastres naturales para asegurar la disponibilidad de seguros y reaseguros asequibles, mitigar interrupciones y garantizar la rápida recuperación. 9. Fomentar e implementar prácticas de contratación transparentes y sostenibles 12 10. Incentivar fiscalmente el financiamiento y la construcción de sistemas de energía renovable, de cosecha de agua y reciclaje, la utilización de materiales reciclables y de infraestructura segura, accesible y asequible 11. Implantar códigos y prácticas que fomenten y aseguren la reducción de la huella de carbón. 12. Promover la investigación e innovación de tecnologías innovadoras y transformación digital, que promuevan el desarrollo sostenible y resiliente. 13. Promover la planificación, diseño, construcción y operación de obras sostenibles y resilientes al impacto del cambio climático. Integración de Iniciativas y Colaboración . Conscientes de iniciativas de organizaciones regionales e internacionales y lo relevante de integrar las de aquellas con las que se mantiene una visión común, UPADI apoya elementos fundamentales de La Declaración de San Juan 2022 de La Academia Panamericana de Ingeniería, La Declaración Stimson de la ASCE y las del Atlas Partnership for Climate Re-



silient Infrastructure, como lo son: . 1. Intercambios internacionales para promover la colaboración de todos los ingenieros en la planificación, diseño, construcción y operación de obras de calidad, sostenibles y resilientes 2. Confeccionar evaluaciones nacionales de infraestructura para confeccionar informes de referencia que promuevan la calidad óptima en el desarrollo, diseño, financiamiento y construcción de obras. 3. Garantizar el desarrollo, diseño, construcción y operación de obras de calidad con las más altas normativas y directrices para promover una mejor calidad de vida, sostenibilidad, mitigación, adaptación y resiliencia para proteger el medio ambiente y asegurar el bienestar de la humanidad en todos los confines del mundo. 4. Atraer más inversiones y mejores cubiertas de seguros al integrar procesos de calidad total que reduzcan los riesgos a la vida y a la propiedad, preservando así vidas y recursos. . Suscrito en Antigua, Guatemala; durante La Reunión de La Unión Panamericana de Asociaciones de Ingeniería, UPADI, hoy 15 de setiembre del 2023.



Hidrógeno

Autor
Ing. Gustavo Mesorio

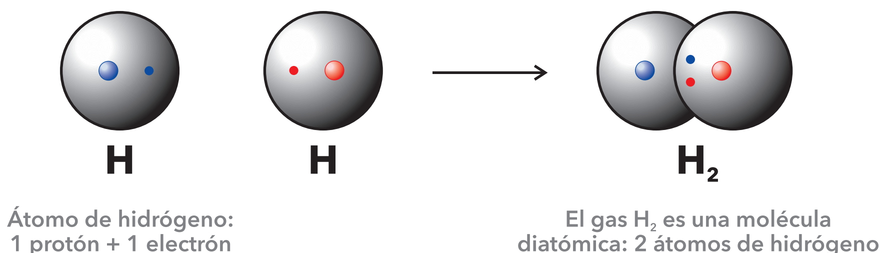
Características del Hidrógeno

Propiedades

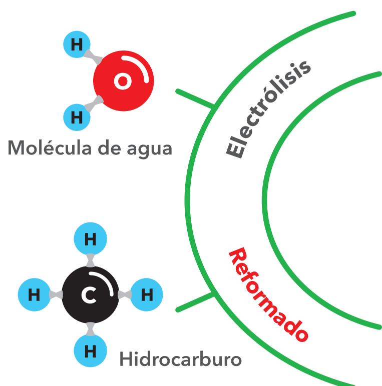
El hidrógeno es el gas más ligero conocido (gravedad específica 0,0695, aire = 1) y se difunde rápidamente en el aire.

Mediante los procesos de Reformado o Electrólisis se puede obtener el Hidrógeno en forma gaseosa.

Con una temperatura y presión estándar, el hidrógeno existe en forma de gas

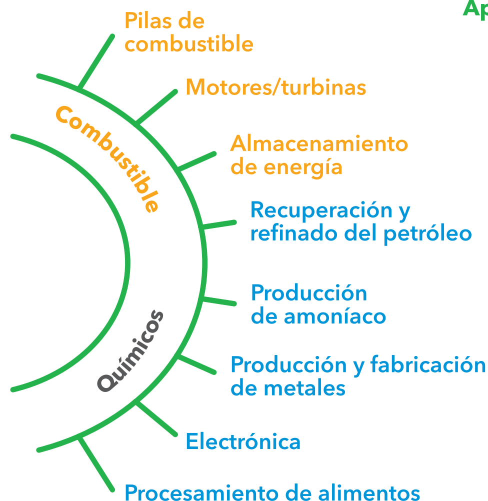


Es el elemento más abundante en el universo pero existe en combinaciones especiales

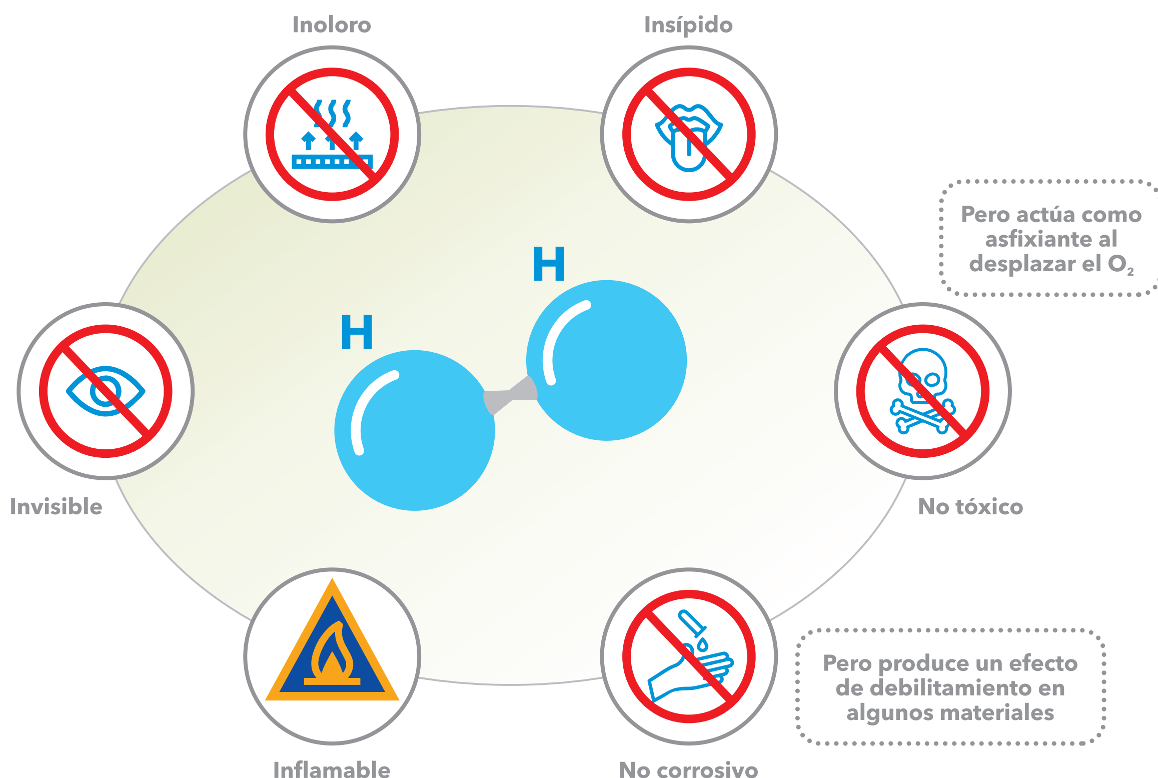


Apenas se encuentra presente en la atmósfera terrestre (0.00005 %)

Aplicaciones



El hidrógeno es incoloro, inodoro e insípido. El hidrógeno no es tóxico, no sustenta la vida y puede actuar como asfixiante reemplazando el contenido de oxígeno en un espacio confinado.

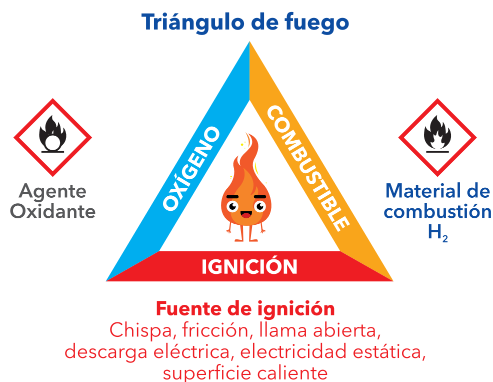


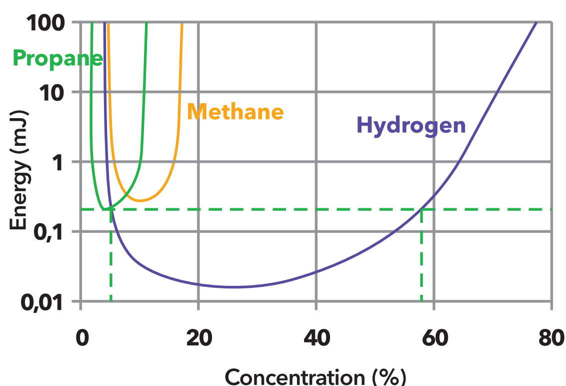
Las principales propiedades del hidrógeno comparadas con otros gases inflamables son las siguientes:

Propiedades	Válido a	Unidades	Hidrógeno	Metano	Propano	Heptano
Punto de ebullición	1,013 bara	°K	20,4	111,6	231,1	371,5
Temperatura crítica		°K	33,19	119,6	396,8	540,4
Presión crítica		bara	13,15	46	42,4	27,5
Densidad del líquido	Punto de ebullición	kg/m^3	70,8	422,5	580,7	680,4
Calor de vaporización	Punto de ebullición	kJ/kg	445,6	510,4	427,8	317
Densidad del gas	Punto de ebullición	kg/m^3	1,338	1,818	2,419	3,29
Densidad del gas	1,013 bara, 0 °C	kg/m^3	0,09	0,717	2,011	4,46
Calor específico, cp	1,013 bara, 0 °C	kJ/kg °K	14,19	2,19	1,56	1,7
Calor específico, cv	1,013 bara, 0 °C	kJ/kg °K	10,06	1,67	1,35	N/A
Conductividad térmica	1,013 bara, 0 °C	W/m °K	0,1682	0,0305	N/A	0,0188
Coeficiente de difusión en aire	1,013 bara, 20 °C	cm^2/s	0,69	0,22	0,12	0,05
Límite de inflamabilidad	1,013 bara, 20 °C	% Vol.	4,0 - 75,0	5,0 - 15,4	2,1 - 9,5	1,11 - 6,7
Temperatura de autoignición	1,013 bara	°C	560	595	470	215
Mínima energía de ignición	1,013 bara, 20 °C	mJ	0,019	0,28	0,26	0,22
Temperatura teórica de llama	1,013 bara, 20 °C	°C	2045	1875	2040	2200

El hidrógeno puede difundirse rápidamente a través de materiales y sistemas que sean herméticos al aire u otros gases comunes. La difusión es más pronunciada a temperaturas elevadas lo que genera un desafío para

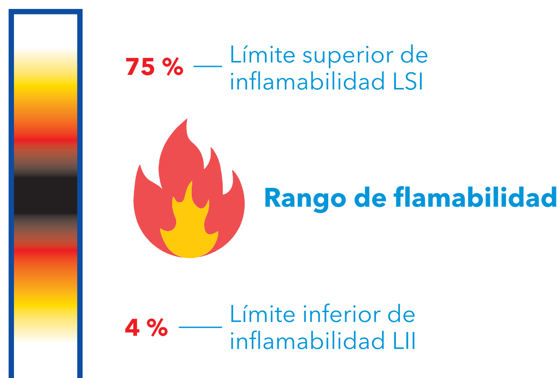
su almacenamiento y transporte. El tamaño de su molécula (muy pequeña) y su baja viscosidad, son factores que inciden en su tendencia a la fuga, situación que se observa más acentuadamente cuando el hidrógeno está bajo presión.





Inflamabilidad

El hidrógeno es extremadamente inflamable en el aire, siendo sus límites de inflamabilidad a presión atmosférica del 4% al 75% en volumen. En mezclas con oxígeno a igual presión, los límites de inflamabilidad van del 4% al 94%.



La energía requerida para encenderlo es extremadamente pequeña, por ejemplo por electricidad estática o fricción de flujo.

La ignición de mezclas inflamables de hidrógeno y aire se produce con un aporte de energía muy bajo, aproximadamente una décima parte del de una mezcla gasolina-aire. Una chispa invisible y/o una carga estática pueden provocar una ignición.

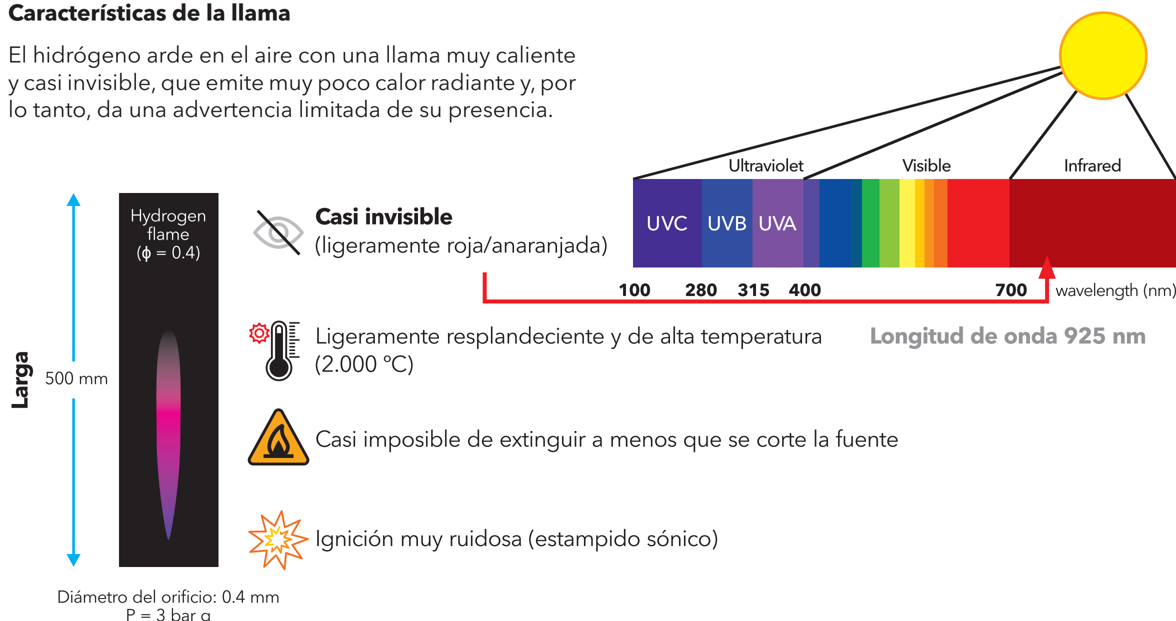
Energía mínima de encendido por chispa en aire: 0,000019 julios (19 µJ)

Energía mínima de encendido por chispa en oxígeno: 0,000017 julios (17 µJ)

Comparando con otros combustibles gaseosos como metano o propano, la energía requerida para encenderse es muy inferior.

Características de la llama

El hidrógeno arde en el aire con una llama muy caliente y casi invisible, que emite muy poco calor radiante y, por lo tanto, da una advertencia limitada de su presencia.



Hidrógeno líquido

El Hidrógeno líquido es mucho más frío que el aire. Su punto de ebullición a presión atmosférica es de -253°C. Recordemos que el cero absoluto es de -273 °C (0 °Kelvin).

El Hidrógeno líquido es uno de los llamados "líquidos criogénicos" nombre con el que se conocen los líquidos a muy bajas temperaturas. Es interesante notar que el Amoniaco (NH3) que se presenta frecuentemente como un derivado del Hidrógeno, tiene una temperatura de ebullición de "solamente" -34 °C lo que facilita su transporte.

El hidrógeno líquido es incoloro e inodoro. Su densidad es una catorceava parte de la del agua. El hidrógeno líquido es extremadamente frío -y a excepción del helio- tiene el punto de ebullición más bajo de todos los gases.

El hidrógeno se compone de orto-hidrógeno y para-hidrógeno. Estas formas tienen diferencias físicas pero no en propiedades químicas. A la temperatura del hidrógeno líquido, el orto-hidrógeno tiende a convertirse en para-hidrógeno. Esta conversión libera calor que favorece la evaporación.

Sin embargo, comercialmente el hidrógeno líquido que se comercializa se compone principalmente de para-hidrógeno.

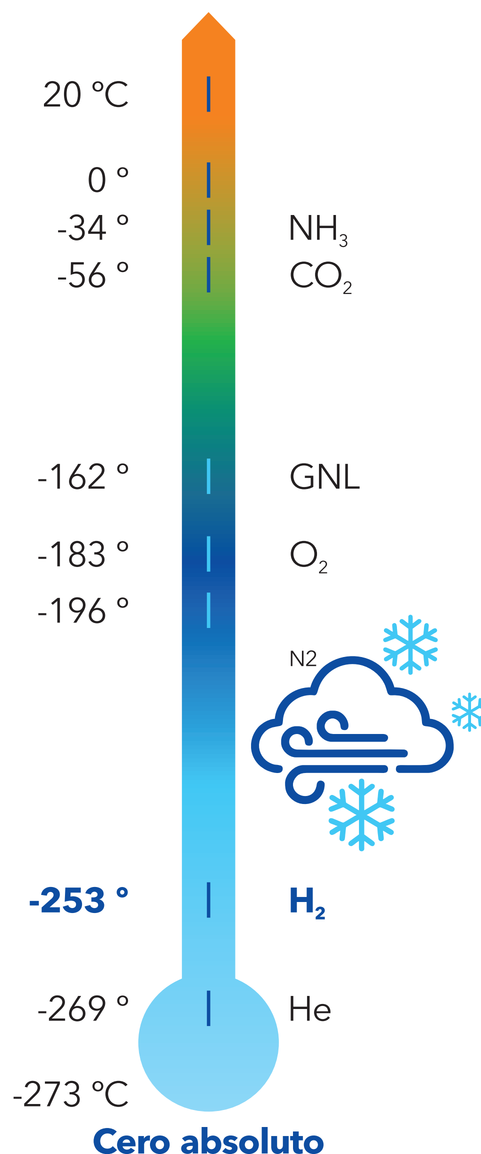
El hidrógeno líquido y el gas frío que se desprende del líquido pueden producir quemaduras graves (similares a quemaduras térmicas) al contacto con la piel. Los tejidos delicados, como los de los ojos, pueden resultar dañados por exposición al gas frío o al líquido salpicado en un breve período de tiempo, que normalmente sería demasiado corto para afectar la piel de las manos o la cara. El contacto entre partes del cuerpo desprotegidas con objetos no aislados de tuberías o recipientes que contienen hidrógeno líquido puede hacer que los tejidos (piel, etc.) se peguen y se rompan.

El hidrógeno líquido y el gas frío que se evapora pueden causar que muchos materiales comunes como el acero al carbono y el plástico o caucho se vuelvan quebradizos y propensos a fracturarse bajo tensión.

A la temperatura del hidrógeno líquido, todos los gases, excepto el helio, se condensan y luego se solidifican. Las partículas sólidas pueden obstruir áreas restringidas, como válvulas y orificios, lo que podría provocar una falla en el flujo y/o aumento de presión. Además, el aire condensado o solidificado en hidrógeno líquido es un potencial peligro de explosión.

El hidrógeno líquido tiene un calor de vaporización muy bajo (en relación con el volumen). Por lo tanto, una pequeña entrada de calor, por ejemplo, la inserción de sólidos o líquidos a temperatura ambiente, creará una evolución violenta de gas y salpicaduras de líquido.

El hidrógeno líquido en contenedores y tuberías mal aislados o sin aislamiento logrará licuar el aire circundante a las mismas. Debido a los diferentes puntos de ebullición del nitrógeno y el oxígeno, el aire condensado está enriquecido con oxígeno y puede causar riesgo de incendio.



El hidrógeno líquido, derramado a la atmósfera, se evapora rápidamente. Un litro de hidrógeno líquido derramado se transforma en aproximadamente 850 litros de hidrógeno gaseoso a temperatura ambiente.

El hidrógeno de ebullición en frío es un poco más denso que el aire y puede acumularse en pozos y zanjas por pequeños períodos de tiempo, dependiendo del volumen derramado y la temperatura ambiente. Luego, rápidamente el hidrógeno asciende y se difunde.

El hidrógeno en ebullición condensa la humedad del aire, creando así una niebla muy visible.

A continuación se presenta una imagen que ilustra los principales peligros que son generales a todos los líquidos criogénicos.



Mecanismo de Explosión

Ya hemos comentado que una fuga de hidrógeno puede encenderse en aire con muy poco aporte de energía. La **combustión** de Hidrógeno es un proceso de oxidación muy rápido y acelerado con producción de llama a baja velocidad. A continuación se presenta una fuga de hidrógeno encendida (combustión de H2). La llama es prácticamente invisible.

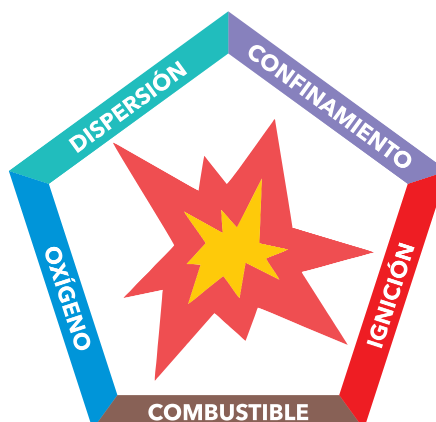


Cuando se produce una liberación de gas hidrógeno que no se enciende inmediatamente, se comienza a formar una mezcla hidrógeno - aire que en algún momento puede alcanzar el rango de inflamabilidad (Hidrógeno en aire entre 4 % y 75 %). Si una nube de esa mezcla se enciende, nos podemos encontrar con dos posibles escenarios de combustión, **la deflagración y la detonación**.

Llamamos **deflagración** a una combustión súbita, en el que la llama viaja a través de la mezcla hidrógeno - aire a velocidades subsónicas (entre 1 m/s y la velocidad del sonido). Las reacciones que provoca la deflagración son similares a las de una combustión, pero se desarrollan a velocidades mayores.

Una deflagración ocurre cuando se enciende una mezcla no confinada de hidrógeno y aire. Una condición no confinada significa al aire libre en un área bien ventilada donde no haya obstrucciones como edificios o paredes.

La **detonación**, es el escenario en el cual la llama y la onda de choque que la acompaña viajan a través de la mezcla a **velocidad supersónica**. **La velocidad de la llama puede aumentar considerablemente con el confinamiento.** Se puede generar una detonación a partir de una deflagración que ha sido encendida en una mezcla confinada o parcialmente confinada.





En próximos artículos seguiremos describiendo los accidentes que se pueden suceder con el hidrógeno y las medidas preventivas y de mitigación que se pueden tomar para prevenirlos o para mitigar las consecuencias si el evento se produce.

Análisis de seguridad de una arquitectura referencial de la plataforma FIWARE

Autores
Ing. Juan Pablo Perata
Facultad de Ingeniería, Universidad de la República, Uruguay
Ing. Gustavo Betarte
InCo, Facultad de Ingeniería, Universidad de la República, Uruguay

I. Introducción

FIWARE [1] es una plataforma de código abierto que surgió en 2011 de una asociación público-privada de la Comisión Europea y la Industria Europea para proporcionar un ecosistema de innovación que permita la materialización de ideas y la creación de aplicaciones y servicios en la nube para múltiples propósitos. Estas características hacen que la plataforma sea de especial interés en el ámbito de las ciudades inteligentes (CI), garantizando la interoperabilidad entre las soluciones desarrolladas y posibilitando su implantación en múltiples ciudades.

La tecnología aplicada al desarrollo de las CI revela, por un lado, una serie de desafíos en materia de seguridad, y por otro, la necesidad de garantizar a los ciudadanos la privacidad de su información. La plataforma de CI comienza a visualizarse como un elemento decisivo al que asegurar y proteger. Esta investigación surge de la motivación de intentar dar respuesta a algunas preguntas que nos planteamos, entre las que destacamos las siguientes: ¿existen vulnerabilidades conocidas en FIWARE? ¿Cuál es el estado de seguridad de los componentes de Fiware a la fecha? ¿Qué exigencias en términos de seguridad impone la plataforma? ¿Es posible desplegar una solución FIWARE insegura?

En este artículo, presentamos los resultados de realizar una evaluación de seguridad de la tecnología FIWARE desde un punto de vista de configuración arquitectónica de sus componentes. El objetivo general del trabajo fue desarrollar herramientas metodológicas para llevar a cabo un análisis de este tipo y, en particular, adoptando una postura ofensiva en la búsqueda, y eventual explotación, de potenciales vulnerabilidades.

La estructura del resto de este artículo es la siguiente: la Sección II describe el enfoque metodológico adoptado en el trabajo que se reporta. La Sección III presenta antecedentes y describe el trabajo relacionado. La Sección IV expone las principales problemáticas de seguridad en plataformas que contienen componentes centrales de toda arquitectura FIWARE. La Sección V describe el modelado de amenazas y análisis de ataque en el escenario referencial. Por último, la Sección VI describe las conclusiones y reflexiona sobre oportunidades de trabajo a futuro.

II. Enfoque metodológico

Se ha realizado una revisión de la literatura de investigación y documentación oficial sobre FIWARE, procurando identificar, entender los desafíos y problemáticas de seguridad en sus componentes y en el despliegue de arquitecturas en distintos escenarios reales descritos en la bibliografía. Asimismo, se experimentó con arquitecturas de ejemplo de FIWARE en una realidad de contexto ficticia para tener un mejor entendimiento.

Uno de los resultados principales presentados en este artículo lo constituye un modelo de amenazas en una plataforma referencial que incluye componentes centrales de FIWARE y que involucra varios artefactos, entre ellos, un diagrama de flujo de datos (DFD), un modelo de de amenazas y la identificación de objetivos de ataque.

La metodología utilizada está basada en el enfoque OWASP para el modelado de amenazas [2], la que propone un encuadre de trabajo metodológico para identificar, cuantificar y abordar los riesgos de seguridad asociados desde una perspectiva ofensiva. En nuestro trabajo, el foco del proceso de modelado está puesto en los siguientes puntos incluidos en los primeras dos etapas anteriores: i) **descomposición de la aplicación desde la perspectiva de un atacante potencial**, ii) **identificación de amenazas con STRIDE** [3], metodología desarrollada por Microsoft que ayuda a distinguir amenazas clasificándolas en 6 (seis) categorías, y iii) **exploración de objetivos de un atacante en activos críticos**. También se han explotado algunos de los objetivos identificados, experimentando en un entorno controlado localmente.

El enfoque dado en la plataforma referencial se validó mediante la realización de un análisis exploratorio de una plataforma FIWARE productiva y real. Eso dio lugar a la identificación de potenciales ataques y a un conjunto de recomendaciones para mejorar la seguridad de varios componentes de esta plataforma.

III. Antecedentes y trabajo relacionado

Unos de los primeros llamados de atención sobre la seguridad de la plataforma objeto de análisis fue comunicado en [4], donde se reporta un *bug* de *race condition* en el componente Orion Context Broker que provocaba el envío de notificaciones a un *endpoint* distinto al esperado. Dicho fallo fue solucionado en 2014 por el equipo de FIWARE.

En [5] los autores utilizan FIWARE como plataforma base en el despliegue de una solución de monitoreo de pacientes de forma remota, donde su principal contribución se centra en aspectos arquitectónicos y de diseño de la misma utilizando componentes de FIWARE denominados *Generic Enablers* (GE) que facilitan la comunicación con diferentes dispositivos IoT e interfaces de interacción con los usuarios. Si bien el estudio se centra en aspectos funcionales, resalta la importancia de la seguridad, en particular la confidencialidad de la información. Describe brevemente la capa de seguridad implementada compuesta por tres componentes: *Identity Management GE* (IdM) que provee mecanismos de autenticación, *Policy Enforcement Point* (PEP) responsable del control de acceso a los recursos en la plataforma y *Policy Decision Point* (PDP) que interactúa de forma directa con el IdM y PEP para brindar una decisión de autorización (permitir o denegar). Cada uno de estos componentes tiene su implementación FIWARE de referencia.

En [6] se presenta el resultado de realizar un análisis de seguridad de FIWARE enfocado en el control de acceso y confidencialidad. Los autores afirman que a pesar de ser una plataforma robusta, algunos de sus componentes tienen muy pocos o ningún mecanismo de seguridad desarrollado. En particular, destacan la ausencia de control de acceso en ciertas operaciones del modelo IDAS 5 y la falta de soporte de cifrado de comunicaciones NGSI para algunas implementaciones de IoT Agent. IDAS es la implementación de referencia FIWARE del componente GE Backend Device Management, que generalmente se usa en la mayoría de los escenarios en la arquitectura IoT.

Dos grupos de investigadores de diferentes universidades europeas [7] y [8] presentan la implementación de componentes de autorización basado en FIWARE, integrando AuthZForce y KeyRock. Los proyectos se centran en aspectos funcionales y están orientados a un caso de uso particular, en un caso una red de electricidad inteligente y en otro el uso compartido y autorizado de datos en ecosistemas industriales. Ambos proporcionan definiciones de alto nivel de políticas XACML para el control de acceso basado en roles.

En [9] se conduce un proyecto de construcción de una plataforma de CI utilizando el stack de componentes de FIWARE. Se presentan los desafíos que conlleva la incorporación de mecanismos de control de acceso a los componentes de la plataforma y sensores IoT.

En [10], los autores presentan un análisis indicando que FIWARE solo admite autenticación pero no autorización para dispositivos IoT, por lo que las credenciales de un sensor comprometido podrían usarse para simular mediciones provenientes de otros sensores. Por otro lado, el trabajo también menciona problemas de seguridad en el modelo multi-tenancy que podrían permitir modificaciones no autorizadas a otro tenant.

Por último, en [11] y [12] los investigadores realizan un análisis global de amenazas de seguridad en CI desde el punto de vista de los dispositivos, sistemas y redes de comunicación. Enumeramos amenazas que tienen relación con este trabajo: accesos no autorizados, spoofing de identidad, ataques man-in-the-middle (MiTM), escucha de comunicaciones, alteración y falsificación de mensajes, software desactualizado.

En base a lo relevado, se destaca que existen muy pocas publicaciones que afronten una evaluación de seguridad de los componentes de FIWARE de forma individual o como un todo en una arquitectura dada.

IV. Problemáticas de seguridad

Contando con un conocimiento básico de los componentes de FIWARE, y habiendo realizado pruebas de concepto interactuando y observando el comportamiento de varios de sus módulos, el siguiente paso dio lugar a profundizar en el análisis de problemáticas de seguridad. Consideramos despliegues de plataformas FIWARE ficticias basadas en tutoriales existentes proporcionados por FIWARE, que contienen componentes centrales de toda arquitectura FIWARE: Orion y IoT Agent.

A continuación se enumeran las principales problemáticas de seguridad identificadas en la plataforma FIWARE que surgen de la revisión de antecedentes, indagación de la documentación oficial y la interacción con los componentes en un entorno controlado local. El estudio estuvo focalizado en los componentes centrales Orion, IoT Agent y sus interacciones:

- No se exige el uso de comunicaciones cifradas TLS entre componentes. Esto posibilita la inspección y/o alteración de datos en tránsito.
- No se exige autenticación con MongoDB. Esto podría posibilitar modificaciones anónimas no autorizadas.
- Versiones de la librería iotagent-node-lib menor a 2.12.0 no soportan autenticación con MongoDB.
- Versiones de la librería iotagent-node-lib menor a 2.13.0 no soportan comunicaciones TLS con MongoDB.
- Versiones de Orion menor a 2.3.0 no soportan TLS con MongoDB.
- Orion no soporta verificación de certificados TLS con MongoDB. Esto podría permitir ataques MiTM entre Orion y MongoDB y que no sean detectados.

- El modelo multi-tenancy podría habilitar modificaciones no autorizadas en otros tenants.
- Los agentes IoT reciben medidas de dispositivos no registrados. Un envío de mediciones de forma masiva en grandes dimensiones podría causar fallas de funcionamiento en el IoT Agent u Orion, provocar indisponibilidad de los servicios o agotamiento de recursos de almacenamiento en MongoDB.
- Orion permite que aplicaciones puedan suscribirse ante cambios de contexto y sean informadas cuando ocurren variaciones. La creación de suscripciones admite una URL arbitraria y condiciones que se tienen que cumplir (por ejemplo en términos de valores de atributos y tipos de las entidades) para que se dispare el evento de notificación. Cuando todas las condiciones especificadas para una suscripción son satisfechas, Orion crea una solicitud HTTP POST sincrónica a la URL especificada con la actualización de los datos en formato JSON. En este sentido, las operaciones de creación, actualización y listado de suscripciones pueden suponer divulgación de información sensible (datos de contexto y aplicaciones existentes suscriptas), si su acceso no es controlado o los mecanismos de control de acceso son permisivos.
- Las cuentas de sensores creadas a través del componente FIWARE IdM Keyrock y utilizadas por dispositivos IoT solo brindan soporte para autenticación pero no autorización. Se plantea un escenario de ataque en el cual si las credenciales de un sensor fueran comprometidas, podrían ser utilizadas para simular medidas provenientes de otros sensores. Asimismo, sería posible generar medidas de sensores inexistentes.

Las problemáticas de seguridad señaladas permitieron establecer un estado de seguridad general primario de los componentes centrales de FIWARE, estudiados a nivel arquitectónico. Esto proporcionó elementos de interés para el comienzo de la etapa de modelado de amenazas en la Sección V.

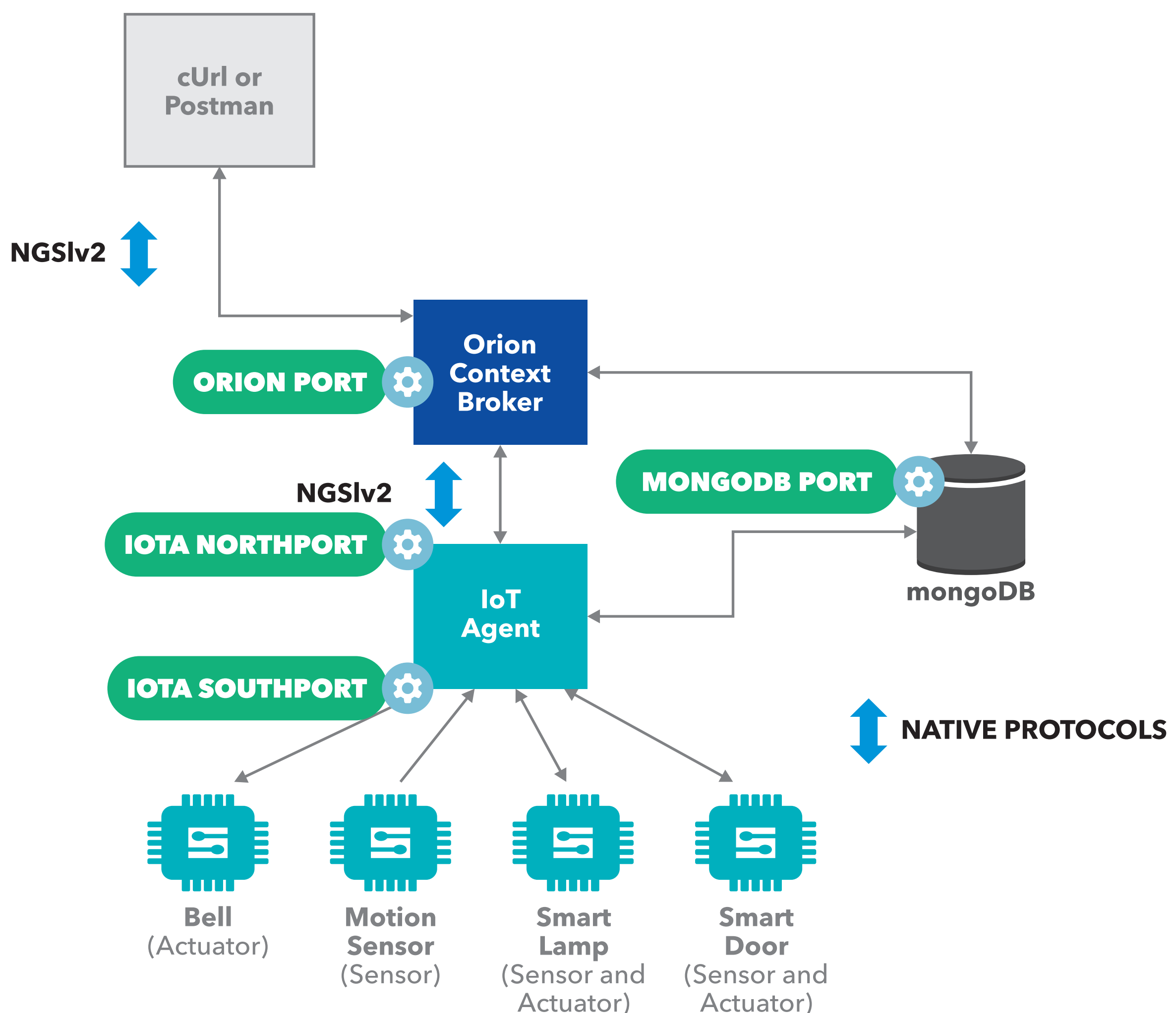


Fig. 1 Plataforma referencial FIWARE [15]

V. Análisis de amenazas y ataque de la tecnología FIWARE

FIWARE proporciona lineamientos de posibles arquitecturas referenciales para que una plataforma sea considerada Powered-By-Fiware. Sin embargo, no exige adherirse a estructuras fijas de despliegue, siendo la única excepción el uso del componente Orion. Los tutoriales de FIWARE modelan una realidad ficticia y están construidos con fines de experimentación y aprendizaje. La documentación menciona explícitamente que no están preparados para ser utilizados como instalaciones productivas, ya que presentan varias fallas de seguridad como credenciales de texto claro, comunicaciones no encriptadas y ausencia de autenticación de base de datos, entre otros. Por otro lado, fue difícil encontrar documentación oficial relacionada con las pautas de hardening con respecto a los componentes FIWARE en entornos productivos.

Esta sección describe el enfoque utilizado para modelar amenazas en una plataforma FIWARE referencial.

A. Plataforma objetivo

El escenario de experimentación es mostrado en la Fig. 1, el cual está basado en un tutorial existente de FIWARE con el fin del entendimiento de la plataforma; se trata de un escenario sencillo que describe una aplicación de manejo de stock de una cadena de supermercados. Consiste en un despliegue simple de microservicios

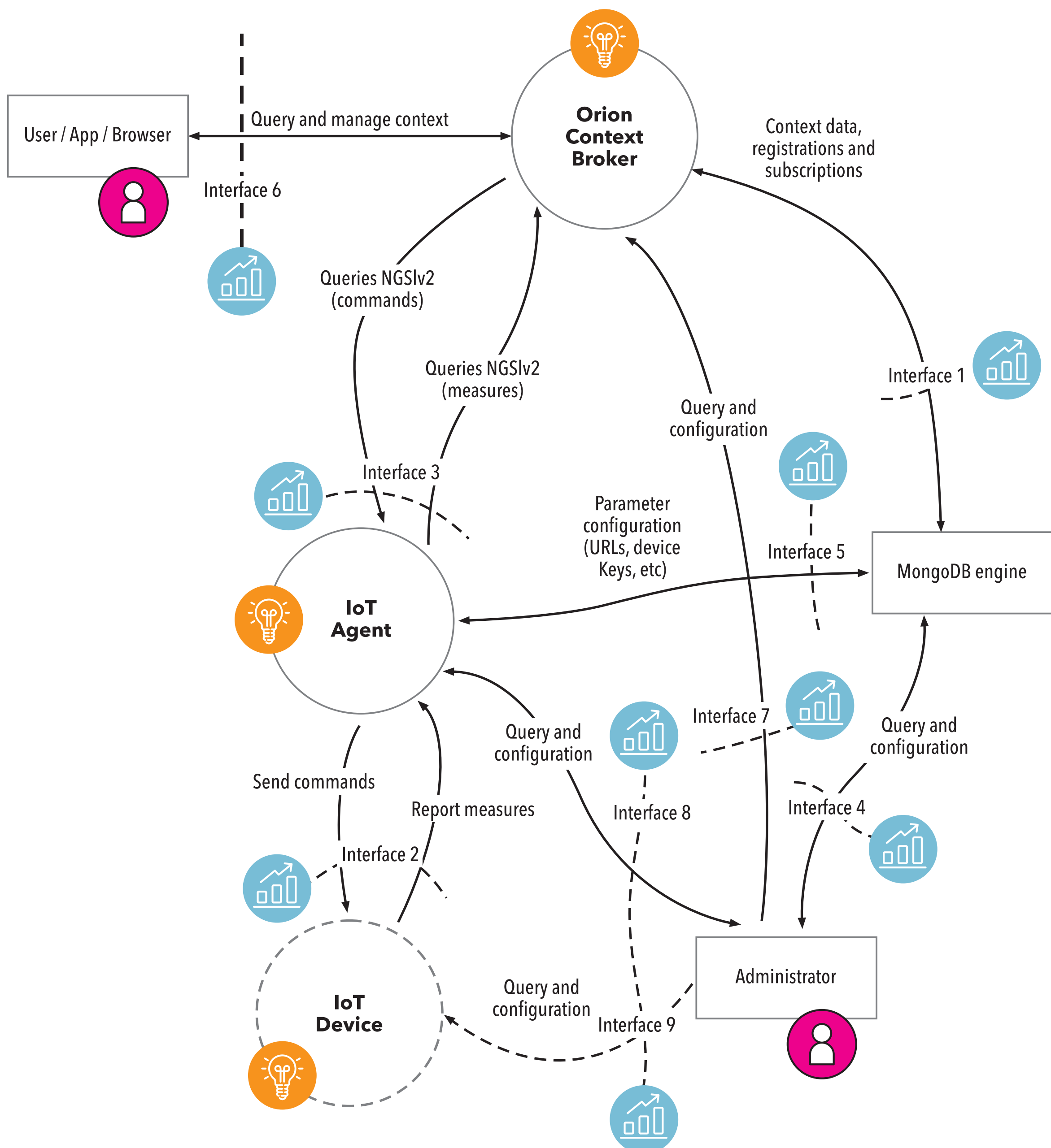


Fig. 2 DFD de la plataforma referencial FIWARE (elaboración propia)

presentes en cualquier plataforma FIWARE, compuesto por varios módulos: i) una unidad central llamada ***Orion Context Broker*** responsable del ciclo de vida de contexto de la información de una realidad imaginaria; proporciona una API RESTful mediante la cual aplicaciones, servicios y otros componentes pueden utilizar para consumir, efectuar cambios de contexto o realizar configuraciones, ii) un artefacto llamado ***IoT Agent*** encargado de permitir que dispositivos con sus protocolos nativos se puedan comunicar con Orion, iii) un motor NoSQL **MongoDB** encargado de las bases de datos vinculadas con estos dos elementos anteriores, y iv) un conjunto de **dispositivos IoT** simulados por software, del tipo sensores (envían medidas) y actuadores (reciben comandos).

Orion es una implementación C++ de la API REST NGSIv2 [13], basada en la especificación OMA-NGSI 9/10 [14], que proporciona un modelo de datos de contexto en torno al concepto de entidades. Mediante solicitudes HTTP es posible crear, ver, modificar y eliminar entidades y atributos relacionados con dichas entidades. Asimismo, proporciona capacidades para listar, registrar, actualizar y eliminar proveedores de contexto de origen externo, así como también listar, crear, actualizar y eliminar suscripciones ante cambios de contexto. Se puede acceder a la API a través de un puerto HTTP, cuyo valor por defecto es 1026.

El componente IoT Agent expone dos puertos, denominados, puerto norte (*northport*) que se utilizará para configuraciones y comunicaciones recibidas del Context Broker, y puerto sur (*southport*), para recibir medidas de dispositivos IoT, cuyos valores por defecto son 4041 y 7896 respectivamente.

Mediante la herramienta *OWASP Threat Dragon* [16], se creó una representación visual de la plataforma en forma de DFD que se muestra en la Fig. 2, donde se pueden encontrar los siguientes componentes: i) **Actores internos y externos**; usuarios anónimos o aplicaciones que interactúan directamente con Orion, y administradores capaces de realizar configuraciones en todos los componentes, ii) **Subsistemas**; señalados por Orion, IoT *Agent* y dispositivos IoT, iii) **Almacenamientos**; ilustrado por el motor MongoDB donde la información se almacena en bases de datos, iv) **Puntos de entrada y salida**; lugares donde potenciales atacantes pueden interactuar con el sistema y donde los datos abandonan el mismo respectivamente: puerto HTTP Orion, puertos norte y sur del agente IoT, puerto MongoDB, *shells* interactivas con Orion y el agente IoT, v) **Barreras de confianza**; denotado por las interfaces definidas a través de puntos de entrada y salida, vi) **Activos**; reconocidos como recursos valiosos para un potencial atacante y que requieren protección: Orion, datos de contexto, IoT Agent, motor y bases de datos MongoDB, ajustes de configuración de cada componente, subsistema docker, credenciales de identificación y autenticación del personal administrativo, vii) **Dependencias externas**; identificado por el motor MongoDB y el subsistema Docker, y viii) **Flujos de datos**.

B. Modelado de amenazas con STRIDE

STRIDE define una clasificación de amenazas en estas 6 categorías: i) ***Spoofing*** es el acto de suplantar o realizar acciones en nombre de un actor o proceso; afecta la propiedad de seguridad de autenticación, ii) ***Tampering*** se refiere a un acto intencional y no autorizado de realizar modificaciones de la plataforma; afecta la integridad, iii) ***Repudiation*** refiere a negar la responsabilidad de una acción; afecta la propiedad de no repudio, iv) ***Information disclosure*** implica la exposición de información a un actor o proceso no autorizado; afecta la confidencialidad, v) ***Denial of service*** alude a provocar que un servicio no esté disponible; afecta la propiedad de disponibilidad, y vi) ***Elevation of privilege*** señala el hecho de adquirir capacidades para un proceso o actor sin la debida autorización; afecta a la propiedad de autorización.

Teniendo en cuenta que el foco del estudio es la plataforma FIWARE, los dispositivos IoT y el flujo de datos provenientes del Administrador quedan por fuera del alcance del análisis de amenazas. Hemos identificado más de 30 (treinta) amenazas en [17], de las cuales se enumera un subconjunto en la Tabla 1, considerando potenciales debilidades que pueden ser explotadas de acuerdo al DFD obtenido en la Subsección A. Vale la pena aclarar que cada amenaza tiene indicada su categoría en la columna Tipo con una letra del conjunto {S,T,R,I,D,E}; cada una representa la primera letra de las 6 categorías STRIDE mencionadas. Procederemos a explicar brevemente algunas de las amenazas identificadas que tienen relevancia para el análisis de ataque que se presenta en la siguiente Subsección C.

ID	Amenaza	Tipo	Interfaz en DFD
T1	Orion malicioso o falso	S	I1, I3, I6
T2	Atacante suplantando identidad de un administrador	S	I4, I7, I8
T3	Alteración de datos en tránsito entre Orion y MongoDB	T	I1
T4	Alteración de datos en tránsito entre IoT Agent y dispositivos IoT	T	I2
T5	Orion impostor suplantando identidad de instancia legítima	R	I1, I3, I6
T6	Escucha de comunicación entre Orion y MongoDB	I	I1
T7	Divulgación de registros de base de datos MongoDB	I	I1, I4, I5
T8	Divulgación de información de contexto y configuraciones	I	I4, I5, I6
T9	Orion no disponible o no respondiendo	D	I3, I6
T10	Acceso no autorizado a Orion	E	I6, I7

Tabla 1. Clasificación de amenazas utilizando STRIDE - Subconjunto de amenazas relevantes.

Las amenazas T1 y T2 se relacionan con actividades de suplantación de identidad. T1 implica la acción de sustituir una instancia legítima de Orion con una versión modificada que actúa como el Orion real pero tiene un comportamiento malicioso intencionado. La amenaza T2, por su parte, representa el acto de realizar tareas en la plataforma con capacidades de un usuario administrador. Las amenazas T3 y T4 muestran casos en los que un atacante potencial puede inspeccionar y modificar el tráfico en tránsito entre componentes de forma no autorizada. La amenaza T5 constituye una amenaza de repudio, donde una instancia falsa de Orion ha ocupado el lugar de la genuina, y es difícil o incluso imposible reclamar la responsabilidad de sus acciones, ya que la actividad legítima frente a la maliciosa no se distingue fácilmente o las tareas maliciosas permanecen desapercibidas. Las amenazas T6, T7 y T8 se refieren a acciones de divulgación de información: T6 identifica la presencia de un MiTM en el tráfico sin cifrar entre Orion y MongoDB, que puede capturar todos los datos en tránsito con la base de datos; T7 hace visible una posible fuga de datos de contexto de los ajustes de configuración directamente desde la base de datos, mientras que T8 refleja el punto de divulgación de información a través de endpoints finales de las API de los componentes. La amenaza T9 supone una instancia de Orion no disponible causada por una acción malintencionada. Finalmente, la amenaza T10 refleja un acceso a Orion de forma no autorizada para tomar control de sus acciones o realizar otros movimientos.

C. Análisis de ataque

En un primer paso de la exploración, decidimos llevar a cabo la identificación de vectores de ataque para los activos de la plataforma que consideramos juegan un papel central en la tecnología FIWARE: Orion y los datos de contexto.

Derivamos, usando las amenazas obtenidas en la Subsección B, los objetivos de ataque que se resumen en la Tabla 2.

ID	Activo	Objetivo de un atacante	Propiedades de seguridad afectadas
O1	Orion	Suplantar la identidad de Orion con una versión modificada	Autenticación, no repudio, integridad, confidencialidad
O2	Orion	Acceso no autorizado	Autorización
O3	Orion	Escapar el contexto de docker y acceder al *host*	Autorización
O4	Orion	Degradar el servicio o indisponibilizar su operativa	Disponibilidad
O5	Datos contexto	Modificación no autorizada	Integridad, no repudio
O6	Datos contexto	Divulgación de datos	Confidencialidad

Tabla 2. Análisis de ataque: identificación de objetivos de ataque para activos críticos Orion y datos de contexto.

Posteriormente, se procedió a experimentar con estrategias ofensivas que nos permitieran afectar la seguridad de los objetivos de ataque identificados. En particular, apuntamos a los objetivos O1, O2 y O6. La idea era experimentar con vectores de ataque remotos o adyacentes a la red de baja complejidad. En la Tabla 3 se presenta un breve resumen de las estrategias de ataque y sus objetivos de ataque correspondientes.

Para el desarrollo de los ataques se utilizaron las siguientes técnicas y procedimientos principales:

- Conocimiento de construcción de imágenes docker.
- Creación de scripts en bash.
- Generación de reverse shells en Linux.
- Conocimiento de técnica SUID para escalación de privilegios en Linux.
- Uso de tcpdump, cliente mongodb.

Las estrategias de ataque A1, A2 y A3 se basan en una posible suplantación de identidad de Orion mediante la modificación de su imagen base. Para comenzar, estudiamos las posibles técnicas que se pueden utilizar para sustituir una instancia de Orion en ejecución aprovechando la generación de una imagen docker maliciosa y poniéndola a disposición en un docker registry que se confía. Identificamos 4 (cuatro) escenarios potenciales en los que podría ocurrir una suplantación de identidad de Orion: (i) una versión modificada y distribuida de la imagen a través de la cuenta oficial FIWARE en Docker Hub, (ii) una versión modificada y distribuida de la imagen creada por una organización y distribuida en Docker Hub, (iii) una versión modificada y distribuida de la imagen creada por una organización en un pipeline de CI/CD y (iv) una versión modificada de la imagen creada directamente en el servidor host o distribuida previamente a un registry local.

El proceso de experimentación siguió la táctica (iv) en un entorno controlado localmente. Si logramos la suplantación de identidad de Orion, demostramos que el uso de la imagen alterada podría permitir:

- Acceso remoto no autorizado a la instancia en ejecución.
- Escalada de privilegios.
- Acceso al motor MongoDB y sus bases de datos sin credenciales aprovechando la ausencia de mecanismos de control de acceso entre Orion y MongoDB.
- Control total de su funcionamiento.

Finalmente, la estrategia A4 proporciona una técnica práctica para filtrar datos de contexto aprovechando que el tráfico entre Orion y MongoDB no se encuentra cifrado.

Conseguimos, por tanto, alcanzar los objetivos de ataque O1, O2 y O6.

ID	Estrategia de ataque	Objetivos de ataque
A1	Imagen modificada de Orion que incluye un proceso en *background* que proporciona un acceso remoto persistente (*backdoor*). Una vez que inicia el contenedor, un proceso realiza periódicamente un intento de conexión a un servidor del atacante para proporcionar acceso mediante consola de comandos.	O1, O2
A2	Imagen modificada de Orion proporcionando un binario SUID para obtener privilegios de root, una vez obtenido un acceso inicial. El binario original /bin/bash es copiado a una ubicación conocida y adicionado el bit SUID.	O1, O2
A3	Imagen modificada de Orion adicionando el cliente mongodb que permite acceso no autenticado al motor MongoDB.	O6
A4	Uso de característica de *docker "network containers"* que permite a un contenedor compartir el stack de red de otro contenedor. Se evidenció que es posible divulgar información entre Orion y MongoDB utilizando un contenedor con tcpdump compartiendo el *stack* de red de Orion.	O6

Tabla 3. Análisis de ataque - Experimentación con objetivos de ataque.

D. Un análisis exploratorio de seguridad de una plataforma FIWARE real

El trabajo de colaboración con los departamentos de TI y Seguridad de la Intendencia de Montevideo (gobierno de la ciudad de Montevideo, capital de Uruguay) (IM), permitió diseñar un análisis exploratorio sobre su plataforma inteligente FIWARE. Como resultado de la realización de un cuestionario guiado, se obtuvo un diagrama representativo de la arquitectura de la plataforma en la Fig. 3.

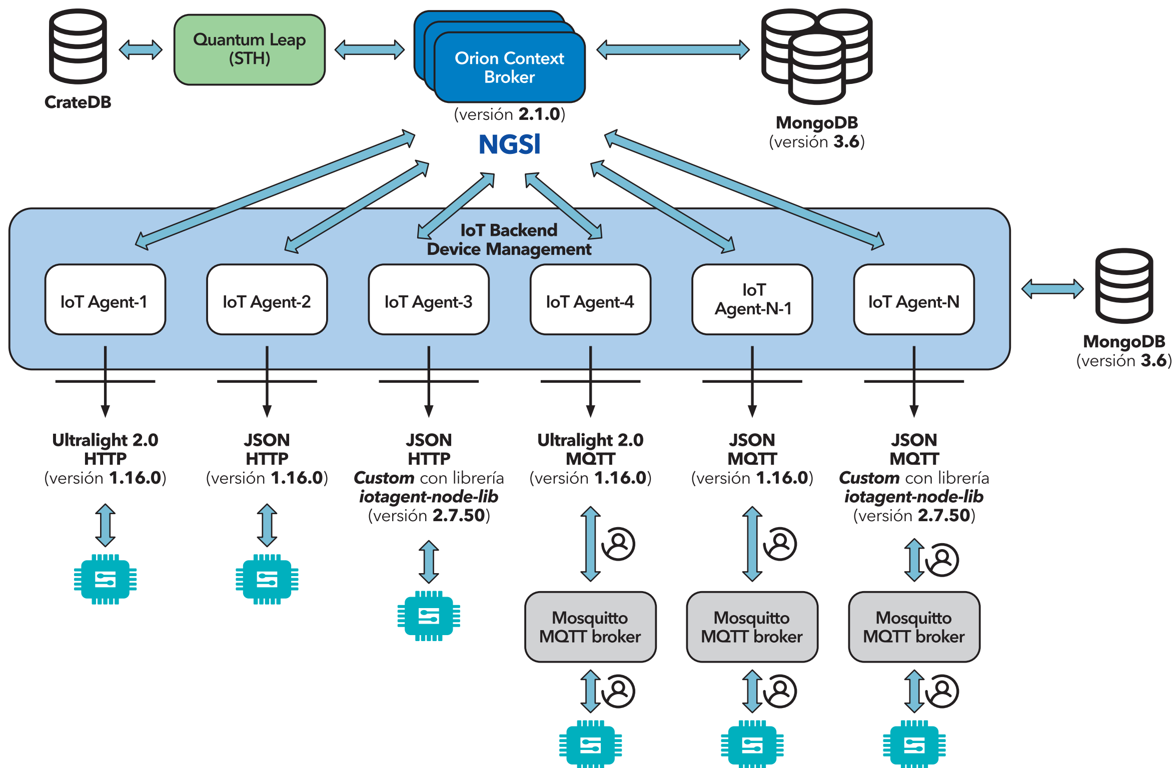


Fig. 3 Escenario de análisis plataforma CI de IM (elaboración propia)

Esta plataforma tiene muchas similitudes arquitectónicas, en términos de su diseño e implementación, con la plataforma de referencia representada en la Fig. 1: es una plataforma de microservicios basada en agentes IoT locales oficiales y personalizados con protocolos JSON y Ultralight, y transportes HTTP y MQTT. Además, los componentes de Orion e IoT Agent no se autentican con MongoDB y las comunicaciones entre los componentes no están cifradas. Las reglas de firewall para el tráfico entrante recibido de dispositivos IoT en los puertos sur no disponen de servidores reverse proxy ni API gateways. A continuación, describimos los resultados del análisis exploratorio de seguridad que hemos llevado a cabo.

En primer lugar, la plataforma utiliza la versión 2.1.0 de Orion, la cual no admite comunicaciones cifradas TLS con MongoDB. En términos de las estrategias de ataque descritas en la Tabla 3, el ataque A4 podría usarse potencialmente para filtrar datos de contexto. Es importante mencionar que se agregó soporte TLS en la versión 2.3.0. En el momento en que se llevó a cabo esta investigación, Orion no admitía la validación de certificados del lado del cliente con MongoDB cuando TLS está habilitado. Esto podría permitir que los ataques MiTM entre Orion y MongoDB pasen desapercibidos. Además, la biblioteca iotagent-node-lib utilizada para los agentes de IoT personalizados estaba en la versión 2.7.50 que no admite autenticación o comunicaciones TLS con MongoDB. Esas capacidades se agregaron en las versiones 2.12.0 y 2.13.0. Se podría usar una estrategia de ataque similar a A4 para filtrar los ajustes de configuración de los dispositivos IoT. Asimismo, todos los agentes IoT comparten el mismo motor MongoDB; eso significa que un IoT Agent personalizado o un usuario anónimo con acceso al motor MongoDB podría potencialmente ver o modificar los ajustes de configuración de una base de datos arbitraria de cualquier agente IoT de forma no autorizada, si combinamos este elemento con dos hechos: (a) autenticación con MongoDB no está configurada, y (b) se usa el nombre predeterminado de las bases de datos. Finalmente, las versiones oficiales de IoT Agent 1.16.0 que se están utilizando en la plataforma permiten el registro de medidas de sensores no registrados. Si un atacante puede interceptar la comunicación entre los dispositivos y agentes de IoT y capturar apikeys válidas (utilizadas para autenticar dispositivos IoT), puede dar medidas falsas de dispositivos reales o incluso medidas de dispositivos no registrados.

El envío de medidas a gran escala podría provocar un mal funcionamiento de IoT Agent u Orion, provocando una denegación de servicio o agotando los recursos de almacenamiento en MongoDB.

Luego de haber realizado el análisis exploratorio de seguridad e identificado vectores de ataque posibles en la plataforma de CI de la IM, se elaboraron un conjunto de recomendaciones y sugerencias en términos de los componentes y sus interacciones.

- Actualizar versión de Orion mayor igual a 2.3.0 con soporte TLS con MongoDB.
- Monitorear las comunicaciones entrantes a MongoDB a fin de identificar comportamientos anómalos, por ejemplo a través del análisis de los mensajes de log. Estas acciones permitirían estar alerta ante eventuales ataques MiTM entre Orion y MongoDB.
- Actualizar librería iotagent-node-lib a una versión mayor o igual a 2.13.0 donde existe soporte para autenticación y comunicaciones TLS con MongoDB.
- Habilitar autenticación con MongoDB en las comunicaciones entre Orion y MongoDB, y IoT Agents y MongoDB.
- Habilitar comunicaciones cifradas entre Orion y IoT Agents, Orion y MongoDB, IoT Agents y MongoDB.
- Proteger APIs expuestas hacia los dispositivos IoT por medio de reverse proxies o API gateways.

VI. Conclusiones y trabajo a futuro

Nuestra investigación proporciona una base metodológica para llevar a cabo un análisis de seguridad de la tecnología FIWARE en cuestión y una identificación de los problemas de seguridad existentes en los componentes FIWARE Orion e IoT *Agent*. El modelado de amenazas basado en STRIDE en la Sección V, Subsección B dibuja un mapa de distintas amenazas, que podría servir como referencia para plataformas similares o más complejas. Es de destacar cada uno de los artefactos resultantes del modelado como ser la descomposición granular del escenario, su representación en un DFD y enumeración de objetivos de ataque de interés para los activos Orion y datos de contexto. Se logró cumplir los 3 (tres) objetivos de ataque propuestos en el escenario de estudio en un entorno controlado; se consiguió fabricar un conjunto de recetas o pasos reproducibles que demuestran su factibilidad. El análisis preliminar de la plataforma real permitió validar y contrastar el análisis de seguridad realizado sobre la plataforma referencial descrita en la Fig. 1.

Múltiples caminos están abiertos para futuras investigaciones que puedan profundizar y enriquecer el trabajo actual. El análisis de seguridad presentado solo cubrió Orion e IoT Agent en una implementación potencial desde una perspectiva arquitectónica. Sería interesante profundizar en las implementaciones de bajo nivel, persiguiendo, por ejemplo, una evaluación de seguridad de la implementación de la API REST NGSIv2 en Orion con el fin de encontrar vulnerabilidades de seguridad y un análisis del código fuente de Orion con foco en el análisis del flujo de datos que puede guiar posibles fallas en el código, como inyecciones y overflows, entre otros. De igual manera que Orion, se podría realizar el mismo abordaje comentado para el componente IoT Agent. Existen además otros módulos referenciales dentro de FIWARE que resuelven aspectos específicos como ser almacenamiento de información histórica, control de acceso, visualización de datos, etc; dichos componentes también podrían ser considerados en un potencial análisis de seguridad.

Referencias

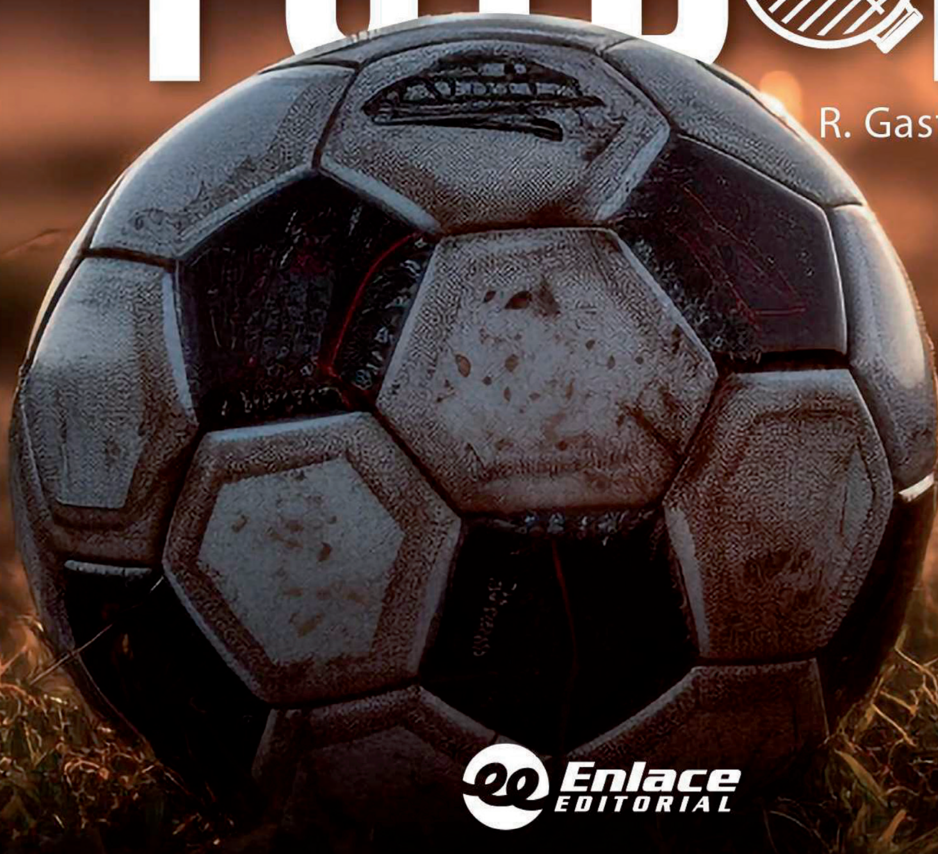
[1] Fiware. 2022. The FIWARE platform. https://www.fiware.org/
[2] OWASP. 2022. OWASP Threat Modeling Process. https://owasp.org/www-community/Threat_Modeling_Process
[3] Microsoft. 2005. The STRIDE security Model. https://docs.microsoft.com/
[4] Santander hackathon. 2013. Github issue: Notification sent to wrong reference endpoint. https://github.com/telefonicaid/fiware-orion/issues/13
[5] Fazio M., Celesti A., Márquez F., Glikson A., Villari M. 2015. Exploiting the FIWARE cloud platform to develop a remote patient monitoring system. https://ieeexplore.ieee.org/document/7405526
[6] C. Thomas Oliveira et al. 2018. Improving Security on IoT Applications Based on the FIWARE Platform. https://ieeexplore.ieee.org/document/8432306
[7] G. Suciu et al. 2020. FIWARE authorization in a Smart Grid scenario. In 2020 Global Internet of Things Summit (GIoTS). https://doi.org/10.1109/GIOTS49054.2020.9119589
[8] Munoz-Arcentales et al. 2020. Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE. Sustainability 12, 9. 2020. https://doi.org/10.3390/su12093885
[9] Salhofer P., Buchsbaum, J., Janusch, M. 2019. Building a FIWARE Smart City Platform. 3-5. https://scholarspace.manoa.hawaii.edu/handle/10125/60175
[10] Peter Detzner and P. Salhofer. 2020. Analysing FIWAREs Platform - Potential Improvements. In 53rd Hawaii International Conference on System Sciences (HICCS). 1–6. https://doi.org/10.1109/SCSP.2016.7501015
[11] Ijaz, S., Shah, M., Khan, A., Ahmed, M. 2016. Smart Cities: A Survey on Security Concerns. 5-11. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.742.883&rep=rep1&type=pdf
[12] Lee J., Kim J., Seo J. 2019. Cyber attack scenarios on smart city and their ripple effects. 2-5. https://ieeexplore.ieee.org/document/8669431
[13] Fiware. 2018. NGSI-v2 Fiware specification. http://fiware.github.io/specifications/ngsiv2/stable/
[14] Open Mobile Alliance. 2012. NGSI Context Management v1. http://www.openmobilealliance.org/release/ngsi/v1_0-20120529-a/oma-ts-ngsi_Context_management-v1_0-20120529-a.pdf
[15] Fiware. 2022. Fiware Tutorial IoT Agent. FIWARE 202: Provisioning the Ultralight IoT Agent. https://github.com/FIWARE/tutorials.IoT-Agent
[16] OWASP. 2022. OWASP Threat Dragon. https://owasp.org/www-project-threat-dragon/
[17] Perata, J. 2022. Análisis de seguridad de la plataforma de ciudades inteligentes Fiware. Tesis de maestría. Universidad de la República (Uruguay). 68-72. Facultad de Ingeniería. https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/33680

MÁS QUE FÚTBOL





R. Gastelumendi



Enlace EDITORIAL

La cultura también presente en la AIU

Autor
Rubén Gastelumendi Puig

Cuento: "A su memoria"

Inauguramos la sección cultural en nuestra revista con un cuento escrito por un asociado de la AIU, ganador de un concurso internacional de cuentos, bajo el seudónimo Rubén Gastelumendi Puig, además autor de la novela "Papifútbol", ver en www.papifutbol.com, ya traducida al portugués y publicada en Brasil, adelantamos que en breve saldrá en Colombia bajo el título "Más que fútbol".

Esperamos nuevos aportes de los lectores, por favor enviar email a aiu@vera.com.uy

Antecedentes: La Comisión de Asuntos Sociales del CAP organizó un concurso literario internacional de cuentos breves, con un máximo de tres carillas en determinado formato, con tema libre, siempre que de algún modo hablara de Peñarol. Quien ganó el primer premio entre más de cien cuentos, es un colega que prefiere conservar el anonimato. Cabe aclarar que el cuento cumple con lo solicitado, pero no es de fútbol, bien podría ser sobre cualquier otro equipo, se trata de la relación que une a dos personas.

A la hora de entregar el premio, el jurado presentó el cuento como *"La recreación de una escena y un diálogo íntimo entre un anciano y un adulto, nos permite atestiguar, como intrusos, qué cosas nutren ese vínculo. El anciano se pierde en su mundo, pero la excusa de hablar de Peñarol sirve para reconectarlos. Así, el veterano recuerda cómo llevaba a su hijo a ver al Chiquito Mazurkiewicz. El cuento, muy apoyado en diálogos y en una escena digna de After Life de Ricky Gervais. Y un final que sorprende, emociona y nos deja un nudo en la garganta".*

A su memoria

Al llegar toqué el timbre y me identifiqué por el portero eléctrico. Se abrió la reja, crucé el jardín hasta la inmensa puerta principal de madera maciza, acorde con aquella enorme casona que fuera una elegante residencia de alguna familia importante de otra época. Aguardé un momento hasta que me recibieron.

–Buenos días. ¿Cómo te va? Adelante, está en el living.

–Gracias –respondí y me dirigí a su encuentro.

Allí estaba, sentado en una vieja butaca mirando distraídamente por la ventana. Su mano derecha en el apoyabrazos, repiqueteaba con un ritmo propio.

–Buen día –. Me acerqué lentamente.

Su vista registró brevemente mi presencia antes de volver su atención a la ventana.

–Buen día –respondió.

–Está muy soleado hoy, ¿no? –comenté, mientras observaba las pocas hojas que conservaban los paraísos a través de la ventana– Pero hace bastante frío... Menos mal que aquí está calentito.

Le dirigí una leve sonrisa y empecé a sacarme la campera y la bufanda. Las colgué en el respaldo de una silla que acomodé a su lado.

–He estado con mucho trabajo.

Su mirada seguía concentrada en la ventana

–Bueno. Es mejor así, ¿verdad? –hice un momento de silencio y continué– ¿Ayer viste el partido de Peñarol?

Una arruga se formó en su frente y se acomodó en el sillón antes de responder.

–No he salido.

–Me refiero, a verlo en la tele.

–No me gusta mirar televisión

Volvió la vista hacia la gran TV colgada de la pared en medio de la sala y agregó:

–Antes no había esas cosas; o iba al estadio o lo escuchaba por la radio.

En la pantalla se mostraban en mute hermosas playas tropicales. La observé por un momento. «Tantas pulgadas, pero no le sirven de mucho» pensé y seguí la conversación.

–¿Ibas seguido al Estadio Centenario?

–Sí– Asintió mirándome–. A mí me gustaba ir todos los fines de semana.

–Ah, ¿sí? Y, ¿qué recuerdos tienes de ese tiempo?

Se llevó una mano a su barba blanca, la mirada perdida buscando en su memoria.

–Llevaba a mi hijo porque quería ver a Mazurkiewicz. Bueno, yo también. –agregó sonriendo– Es que a los dos nos gustaba jugar de arquero.

–A mí también.

Le devolví la sonrisa. Me estudió la cara un momento y siguió:

—Y, si había alguien de quien se debía de aprender, era ¡del Chiquito! Pero claro, ver a Spencer hacer varios goles, era también un gran gusto.

—Parece que esa época la tenés muy presente.

Me acomodé en la silla llevándome una mano al mentón y escuché con interés.

—No sé. Pero de Abbadie, Rocha, Spencer, Joya, Tito y Mazurka no me olvidé. —dijo apuntando satisfecho el dedo índice sobre su sien.

—¡Qué memoria!

Después de un par de minutos en silencio, comenté:

—Me dijeron que conociste a Lucho Borges.

—Sí, lo vi hacer el primer gol de la Copa Campeones de América.

—Ah, sí; de la Libertadores.

—¡Exacto! Fue sobre la Colombes. Jugada de Hohberg, tiro de Cubilla que pegó en el travesaño y Borges agarró el rebote de zurda. A los pocos minutos hizo otro. Después vinieron varios de Spencer.

—¡Qué jugadores!¡Unos héroes!

—Un jugador de fútbol no es un héroe —dijo, negando con la cabeza—. Pero, Lucho sí lo es.

—¿Por qué solo él?

—Por lo del Vapor de la Carrera —respondió como si fuera obvio— ¿Qué pasó? —pregunté sorprendido.

—En julio del 63 —empezó pausadamente, con su voz de narrador—, cuando el barco se dirigía a Buenos Aires chocó, se incendió y comenzó a hundirse en plena noche de niebla. En medio del caos la gente se tiraba al agua helada porque no había suficientes botes disponibles. Lucho con su chaleco salvavidas logró aferrarse a la caja de un violonchelo y, aunque no sabía nadar, logró salvar a un niño arrojado al agua por su madre para evitar las llamas.

—¡Impresionante!

La que me había abierto la puerta estaba cerca y escuchó el relato. Se acercó y en voz baja me dijo:

—Se lo escuché varias veces. Me da curiosidad.... ¿es cierto?

—Por supuesto que lo es. Doy fe que llevaba a su hijo al estadio.

Ella sonrió y se alejó.

Recostado nuevamente en la butaca, su atención había vuelto a la ventana, donde una corriente interminable de coches pasaba por la avenida. Suspiré.

—Esta tarde vendrá mamá a verte, como todos los días.

—¿Quién? —preguntó, ausente.

—Rosa.

No respondió, su mano volvió a repiquetear en el apoyabrazos; su mirada fija en el tránsito.

—Bueno —Vacilé— Me tengo que ir.

Lo miré unos momentos. La barba blanca le relucía en la luz invernal, al igual que el poco pelo lacio que le quedaba en la cabeza. Me pregunté si algún día yo sería tan canoso.

—Tengo que ir a trabajar.

—¿En qué trabaja usted? —preguntó de repente con curiosidad en los ojos.

—En nada importante —respondí mientras agarraba mi abrigo.

—¿Por qué vino? —insistió con su mirada fija en la mía.

Le puse una mano en el hombro y le di un leve apretón con cariño.

—Porque me gusta escuchar tus historias de Peñarol — dije simplemente.

—¡Ah! —Con una sonrisa cordial y su atención volviendo a la ventana, respondió—. Me parece muy bien.

Miré alrededor notando todas las personas que deambulaban en la gran sala, o que conversaban en sus propias butacas, indiferentes a mi presencia.

—¿Listo? —me preguntó la misma funcionaria.

—Sí. Gracias, Raquel.

Crucé el jardín, se abrió la reja y ya en la vereda lo busqué en el ventanal. El reflejo sobre el vidrio me mostraba una imagen distorsionada, pero allí estaba. Aunque no me vio, lo saludé con la mano y le dije bajito:

—Gracias, Pá.

La responsabilidad del Planificador y la encrucijada del Decisor

Autor
Dr. Ing. Prof. Gonzalo Casaravilla



La Planificación de la Expansión de la Generación (PEG) es un ejercicio que debe realizarse periódicamente. Otrora suponía la adopción de decisiones esporádicas de inversiones importantes en dimensión y costo como ser centrales térmicas o represas hidroeléctricas. Esta dinámica definitivamente ha cambiado con la fuerte irrupción de las ERNC. Por una parte, en condiciones de régimen, son inversiones modulares que se pueden ir incorporando año a año. Esto, por otra parte, determina la conveniencia de adoptar decisiones todos los años.

Por ejemplo, tomando como criterio que una vez decidida una inversión de un parque eólico o fotovoltaico alcanzan dos años para disponer de la energía asociada, una buena práctica sería que todos los años se hiciese la PEG de las inversiones que deberán estar operativas en un par de años. En dicho contexto la adopción de una ventana de tiempo decenal para realizar el estudio de inversiones es solo a los efectos de otear el horizonte, y son los primeros años de todo estudio de PEG los relevantes.

Las responsabilidades de los Planificadores son, más allá de utilizar herramientas y modelados que mejor representen la realidad, la caracterización de las hipótesis que determinan los escenarios principales e informar sobre los costos de cada opción. La información a entregar por el Planificador tiene que ser suficiente como para que el Decisor tenga los elementos como para tomar el camino adecuado. En tal sentido y atendiendo a la naturaleza estocástica de los recursos (hidráulica, solar, eólica y combustibles para las térmicas) hace que los resultados de cualquier cálculo o estudio particular se obtienen simulando determinada cantidad de crónicas (suertes) por lo que se obtiene para cada suerte un valor del Costo Futuro (CF).

En la Figura 1 se puede observar el resultado 1000 crónicas simuladas, ordenando los valores de menor a mayor, para un par de escenarios que luego se comentarán. Las curvas de CF así ordenadas caracterizan el Riesgo con su probabilidad de excedencia en el eje horizontal. Por ejemplo, se pueden observar sobre el medio de las curvas los valores esperados (medios) de cada escenario (CF_VE).

De la información así presentada se pueden comparar valores en Riesgo, como es el Riesgo Condicionado (que es el promedio de determinado conjunto de suertes). Por ejemplo, se pueden tomar el 10 % de las peores suertes y el 10 % de las mejores suertes, lo que es respectivamente la evaluación del promedio del último 10 % y del primer 10 % de los CF de las curvas de cada escenario de la Figura 1.

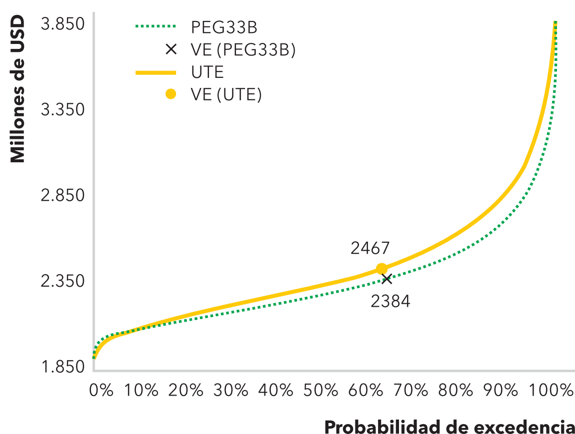


Figura 1. Excedencia de los Costos Futuros acumulados de los años 2024 a 2026[1].

1 Los costos acumulados 2024 a 2026 se calculan con una tasa de descuento del 10 %. Incluye básicamente los costos directos de los años 2024 a 2026 de los variables de las térmicas, los pagos por energía de las ERNC, la valorización de excedentes y el costo futuro a partir del año 2027. Todos los escenarios tienen el mismo costo futuro a partir del 2027.

En suma, el Decisor tendrá escenarios, y para cada escenario un resultado económico, tanto del Valor Esperado, como de la surtes posibles para cada extremo de ocurrencia.

Un resultado que en general ocurre para un Sistema como el de Uruguay, es que las curvas de Riesgo del CF de un sistema con expansión óptima con ERNC y un sistema subequipado se cruzan sobre el extremo de las mejores suertes. De allí la importancia de no solo ver el sobrecosto entre escenarios cuando la suerte es adversa con los recursos o el precio del fósil. Para evaluar correctamente el Costo de Arrepentimiento, también hay que evaluar el ahorro que significaría el no haber hecho la expansión óptima, pero se tenga una buena suerte con las lluvias y el precio del combustible fósil.

Poniendo en números un ejemplo, se analizan algunos resultados del trabajo [4]. En la Tabla 1 se observan las expansiones de cuatro escenarios posibles de expansión en el corto plazo. Los escenarios a comparar son: a) PEG33, que es la Planificación Decenal 2024-2033 realizada el año 2022 por parte de Grupo de Energía Eléctrica de la Facultad de Ingeniería de la UDELAR [1], b) PEG34, que es Planificación 2025-2034 realizada en el 2023 [2], c) ADME, que es la expansión incluida por la Administración del Mercado Eléctrico de Uruguay en su Planificación Estacional de Mayo de 2023 [3], d) UTE, que son las inversiones anunciadas por la empresa eléctrica de Uruguay para los años 2025 y 2026, y finalmente, no incluido en la tabla, e) Base, que es un escenario sin expansión.

En general se analizan y comparan escenarios de expansión suponiendo una Baja Demanda esperada. Los resultados del presente trabajo no incluyen el escenario de Alta Demanda esperada asociada a la efectiva instalación de un Data Center que requeriría una demanda adicional relativamente importante en el corto y mediano plazo.

En todos los escenarios se incluyen los 29 MW que UTE informa estarán operativos en 2024. En todos los escenarios se asume como criterio conservador que se exportan los excedentes energéticos ocasionales a un precio de 12 USD/MWh. Todos los números asociados con costos se refieren a dólares del año 2023 y son el acumulado del CF de los años 2024 a 2026.

AÑO	PEG33B			PEG34B			ADME			UTE		
	MW Eólica	MW Solar	MW-m ERNC	MW Eólica	MW Solar	MW-m ERNC	MW Eólica	MW Solar	MW-m ERNC	MW Eólica	MW Solar	MW-m ERNC
2024	50	250	**76**	0	0	**0**	0	0	**0**	0	0	**0**
2025	50	250	**76**	50	250	**76**	164	502	**178**	0	25	**6**
2026	250	250	**224**	250	550	**224**	214	502	**198**	0	100	**22**

Tabla 1. Inversiones de Generación Eólica y Solar de cada escenario. La tabla no incluye el escenario Base ya que no tiene ninguna expansión.

Luego, en la Figura 2 se observan las energías anuales asociadas a cada escenario de expansión analizado.

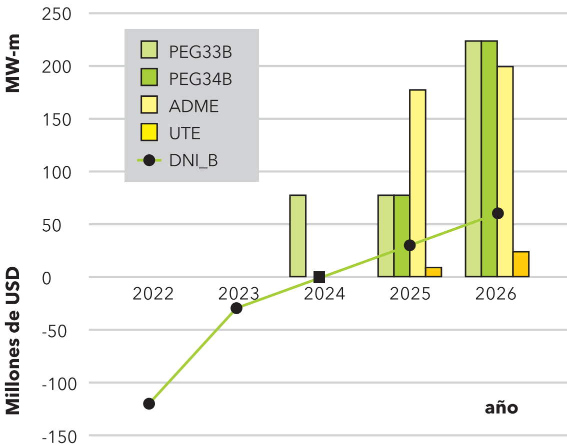


Figura 2. Potencia media de generación (equivalente a energía) de las expansiones de los escenarios comparados y Demanda Neta Incremental (DNI_B) considerando Baja Demanda respecto a la Demanda del año 2024.

El resultado es por una parte, que comparando con el escenario PEG33, los sobrecostos de cada escenario en Valor Esperado son: 16 (PEG34), -3 (ADME), 83 (UTE) y 87 (Base) millones de dólares (Figura 3).

Por otra parte, para el conjunto de 10 % de casos más adversos, el costo promedio se ve incrementado respecto al PEG33 en: 48 (PEG34), -17 (ADME), 279 (UTE) y 289 (Base) millones de dólares (Figura 4). Finalmente, en el conjunto de 10 % de casos más favorables, el costo promedio se ve reducido en: 4 (PEG34), -1 (ADME), 19 (UTE) y 21 (Base) millones de dólares (Figura 5).

Como estudio de sensibilidad de los resultados y atendiendo al hecho de que se está pudiendo comprar excedentes térmicos en la región a precios convenientes, se modeló que los costos de las térmicas se reducen un 35 %. En este caso, los sobrecostos incurridos en Valor Esperado se reducen aproximadamente a la tercera parte, los sobrecostos de casos más adversos se reducen a la mitad, y la reducción de costos de casos más favorables aumentan al doble.

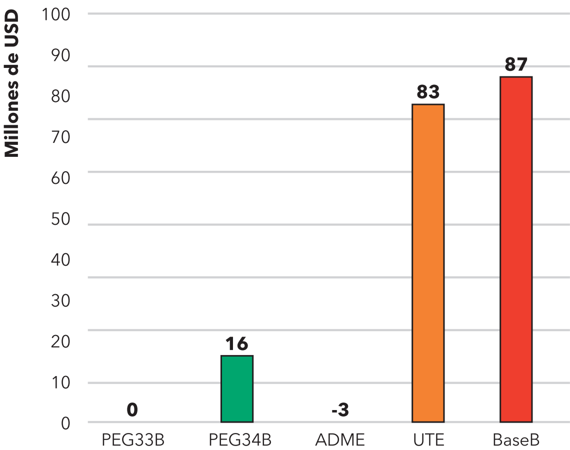


Figura 3. Sobrecostos en el Costo Futuro en Valor Esperado respecto al escenario PEG33B con Baja Demanda. Con Costos Térmicos Normales.

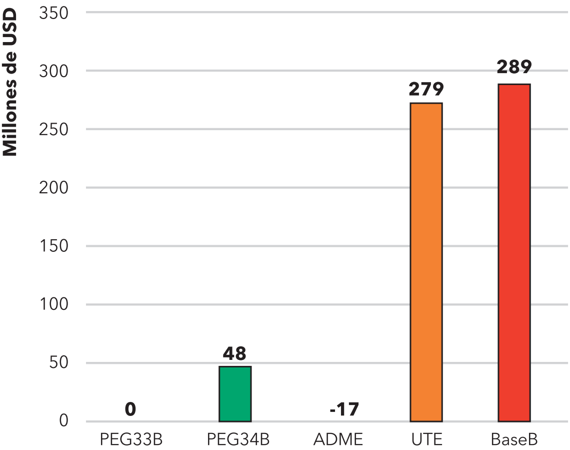


Figura 4. Sobrecostos entre los valores Condicionados de Riesgo de 10 % (promedio del CF del 10 % de peores suertes) con Baja Demanda. Con Costos Térmicos Normales.

En el trabajo [4] se concluye que: "Con las hipótesis consideradas en el estudio, con Baja Demanda esperada, ya se habría incurrido en sobrecostos en Valor Esperado, que difícilmente sean remediables, ya que

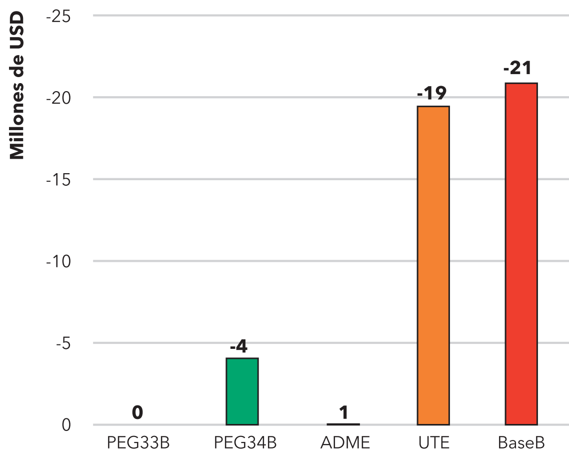


Figura 5. Reducción de costos entre los valores Condicionados de Riesgo de 10 % (promedio del CF del 10 % de mejores suertes) con Baja Demanda. Con Costos Térmicos Normales.

el tiempo que media en Uruguay entre que se decide una inversión de ERNC y la misma está disponible, es al menos de un par de años.

En lo que refiere a comparar las curvas de Riesgo y evaluar los Costos de Arrepentimiento entre escenarios para los casos adversos o favorables considerados, los sobrecostos de los casos más adversos son sensiblemente mayores a los beneficios de los casos más favorables. En el caso de costos de combustible normales, la razón es 15 a 1, y en el caso de costos de combustibles un 35 % más bajos, la razón es 4 a 1.

Asimismo, en el caso de que finalmente se instale el Data Center que en setiembre de 2023 ha sido anunciado, se configuraría un escenario de Alta Demanda esperada, que requerirá acelerar la toma de decisiones para mitigar los sobrecostos y riesgos informados."

Esta es la encrucijada del Decisor. Al final del día, cualquiera sea la decisión que adopte, la misma será objeto de un riguroso análisis en base al "diario del lunes". Pero si el Decisor se apoya evaluando informes técnicos hechos por Planificadores que hicieron su trabajo a conciencia y ambos, Planificadores y Decisores, actúan como si se tratar de plata propia, seguramente el resultado, si bien sujeto a un futuro no del todo cierto, será lo mejor que se hará podido hacer con la información disponible.

Bibliografía

[1] Casaravilla, G y Caporale, X. (2022.). Propuesta metodológica para la planificación decenal de la expansión de la generación de Uruguay. Reportes Técnicos del Grupo de Energía - GEE, vol. 3, no 7, dic 2022, pp. 1-13.

[2] Casaravilla, G y Caporale, X. (2023.). PEG34: Planificación de la Expansión de la Generación Decenal 2025-2034 de Uruguay. Reportes Técnicos del Grupo de Energía - GEE, vol. 4, no. 9, oct 2023, pp. 1-12.

[3] ADME, "Programación estacional mayo-octubre 2023". Mayo 2023.

[4] Casaravilla, G y Caporale, X. (2023.). Sobrecostos acumulados incurridos por retraso de Inversiones en Generación entre los años 2024 y 2026. Reportes Técnicos del Grupo de Energía - GEE, vol. 4, no. 10, nov 2023, pp. 1-7.

Generalidades sobre sistemas de sonido domésticos

Autor
Ing. Javier Beltrame

En el presente artículo detallamos los tipos más frecuentes de sistemas de sonido hogareños, desde el punto de vista de nuestros oídos, dado lo vasto del tema.

Sistemas monofónicos

Como casi todos conocemos, los primeros sistemas fueron monofónicos, es decir un solo canal de información, un solo altavoz o reproductor acústico, comenzando con el fonoautógrafo (1857), fonógrafo (1877), o gramófono (1887). La mayoría de las radios portátiles y unos cuantos celulares continúan siendo monofónicos en cuanto a los parlantes que utilizan, aunque algunos pueden reproducir en forma estereofónica a través del puerto de auriculares, en forma cableada o inalámbrica. También muchos parlantes inalámbricos son monoaurales o monofónicos. Esto evidentemente obedece a que muchas veces, por razones de costo, practicidad, o simplificación en el diseño, o el lugar previsto de escucha, no es estrictamente necesario.

Sistemas estereofónicos o Sistemas 2.0

Canal frontal izquierdo y frontal derecho. Los sistemas estereofónicos o muchas veces llamados 2.0 hoy en día, tienen dos canales independientes de transmisión. La razón más importante para duplicar el procesamiento de la señal se relaciona con la ubicación espacial del sonido, no necesariamente con la calidad de la señal en sí misma. Este punto es importante, dado que por ejemplo podemos citar que la calidad de la señal en un disco vinilo monofónico puede ser superior al mismo en formato estereofónico, simplemente por el hecho de que el mismo formato físico debe almacenar más información. Que exista la posibilidad, por supuesto, no significa que eso sea algo que se reitere en muchos casos.

Se cita al Ingeniero inventor inglés Alan D. Blumlein como el creador del formato estereofónico en 1931 y a la célebre película de Walt Disney, Fantasía (1940), como la primera con dicho adelanto.

https://interestingengineering.com/innovation/alan-dower-blumlein-the-forgotten-engineer-with-128-patents

Los seres humanos tenemos dos ojos y dos oídos, y es fácil comprobar que si nos tapamos un ojo, perdemos la noción de distancia. Sucede algo similar si nos tapamos una oreja, cuesta mucho más individualizar la procedencia del sonido. Por esa razón, hablamos de visión estereoscópica o escucha estereofónica. Nuestro ojo izquierdo no percibe exactamente igual que el derecho y nuestro cerebro aprendió a asignar esa diferencia a la distancia de los objetos. De la misma forma, si estamos sentados frente a una orquesta, nuestro oído derecho no escucha exactamente lo mismo que el izquierdo. En un sistema estereofónico, por lo general, se colocan dos micrófonos para grabar la orquesta o banda, se graban y reproducen sus señales por canales diferentes, de manera que lleguen a nuestros oídos dos señales distintas y permitan recrear la imagen sonora, similar a si estuviéramos presentes en el auditorio. Pero de esta manera, sólo se logra una reproducción adecuada en el espacio comprendido entre los dos reproductores, o parlantes, no fuera de ellos. En sistemas correctamente implementados, el realismo que se puede obtener es notable. Aclaramos que muchos de estos temas son o pueden ser objeto de discusiones, y la intención del artículo es meramente ilustrativa.

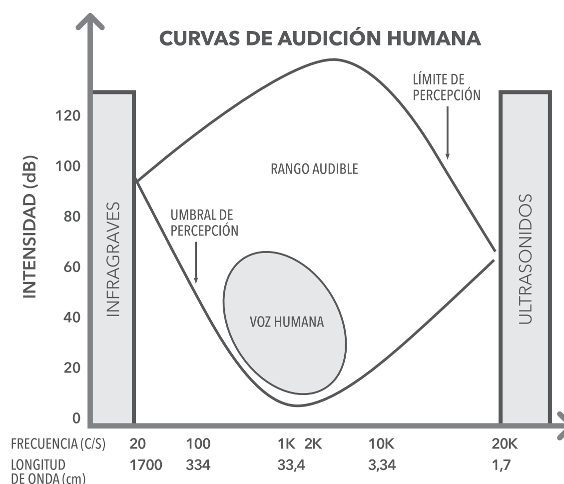


Fig. 1 Curvas de audición humana

La Fig. 1 nos da una idea de la relación entre la sensibilidad de nuestros oídos, la frecuencia y la intensidad de ellos, y como tenemos mayor sensibilidad a las frecuencias de la voz humana. El rango audible generalmente aceptado es de 20 a 20.000 ciclos por segundo para personas jóvenes, o sea longitudes de onda que van desde los 17 m a los 17 mm (1700 a 1,7 cm).

Sistemas 2.1

Constan de 3 canales, uno frontal izquierdo, uno frontal izquierdo, frontal derecho y subwoofer. Estos sistemas utilizan un efecto importante de las ondas sonoras, el hecho de que las frecuencias muy bajas no son direccionales para nosotros. Es decir, no somos capaces de distinguir la procedencia del sonido si la frecuencia es muy baja.

La explicación es la siguiente: Teniendo en cuenta que la velocidad de transmisión del sonido en el aire es de unos 343 m/s aproximadamente, la longitud de onda de sonidos comprendidos entre 20 y 100 c/s es de 17 a 3,43 metros ($\lambda = c / f$). Esto significa que la amplitud y la fase de estas frecuencias es la misma para cualquiera de nuestros oídos, ya que esas distancias son bastante mayores que la distancia entre ellos, o sea que ambos escuchan lo mismo. Es decir, a 100 c/s por ej. la longitud de onda es de unos 3,43 m.

En la práctica, se usan frecuencias de corte entre 80 a 120 c/s para aprovechar este efecto. Esto permite utilizar una sola unidad para la reproducción de las frecuencias más bajas, las cuales son más grandes,y más pesadas, los llamados "subwoofers", y reducir el tamaño y peso de las otras unidades, llamadas en ocasiones "satélites". Estas unidades reproducen el resto del rango de frecuencias por encima de los 100 c/s aprox. hasta los 15.000 o 20.000 c/s. Son muy útiles por ejemplo en casos de sistemas de reproducción para computadoras de escritorio. Podemos citar que en general este tipo de sistemas diseñados para el escritorio, ya incorporan los amplificadores y filtros necesarios.

En sistemas de mayor calidad, una práctica muy usada y de muy buenos resultados, es realizar esta división en frecuencias aún más bajas, por ejemplo 60 c/s. De esta forma se libera a las unidades principales/frontales de las frecuencias más bajas, las cuales requieren mayor energía y desplazamiento de las membranas transductoras y enmascaran el sonido de las voces. También se logra reducir el efecto direccional que en ocasiones se presenta en estas frecuencias.



Fig. 2 Ejemplo de Sistema 2.1 para escritorio



Fig. 3 Ejemplo de Sistema 2.1 de alta calidad

Sistemas 3.1

Canal frontal izquierdo, frontal central, frontal derecho y subwoofer.

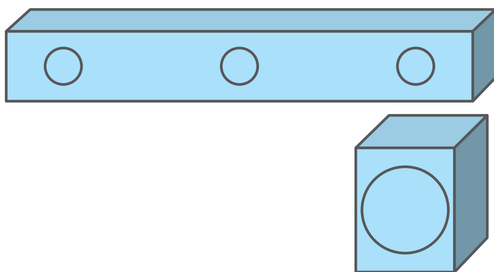


Fig. 4 Ejemplo de barra de sonido 3.1

Estos sistemas generalmente se aplican a las llamadas barras de sonido, dado que incorporan una canal central adicional a los comunes izquierdo y derecho, además del subwoofer. Pero aunque no tan comunes, también hay sistemas con 2 canales frontales, uno central y un subwoofer con unidades tradicionales. Son sistemas adecuados para teatro en casa o mirar TV, ya que el canal central permite una mejora importante en la localización de los diálogos o películas. Para que tenga sentido, la decodificación de la señal es diferente a la común estereofónica, típicamente toman la decodificación 5.1 sin los canales posteriores. Se ha hecho común la forma de denominar los sistemas con el número de canales primero, sean 2,3, 5 o incluso 7 y 9, agregando el .1 (punto 1) para indicar que poseen un subwoofer. Por esa razón, vemos comercialización de sistemas 2.1, 3.1, 5.1, 7.1 y 9.1. Las barras de sonido en sí, desde el punto de vista estrictamente acústico, no incorporan mejoras, sino practicidad y estética. Un problema inherente al diseño es la gran superficie radiante del canal central, frente a la opción de tres unidades frontales separadas. Sin embargo en buena medida en parte a procesamientos de la señales y ajustes en los diseños, se pueden logran resultados muy convincentes. Debemos citar también que muchas barras de sonido, en especial las de gama de entrada o más económicas, en realidad son sistemas 2.0, luego 2.1 al incrementar el precio, 3.1 y algunas incluso incorporan 2 canales posteriores para conformar un sistema 5.1.

Sistemas 3.1.2

Este tipo de barras de sonido incorporan 2 canales adicionales hacia el techo, además de los 3 frontales y el subwoofer. Estos canales adicionales dirigidos hacia arriba, brindan un sonido más espacial, pero nue-

vamente la decodificación de la señal original se debe realizar adecuadamente. Ejemplo de estos sistemas es la decodificación Dolby Atmos (Tecnología de audio basada en objetos) o DTS:X. No debemos confundirlo con Dolby 7.1 por ejemplo, que es una decodificación de sonido envolvente tradicional. En próximos artículos entraremos más en detalle sobre este tema, y cómo la Neurociencia también brinda sus aportes para lograr realismos en ocasiones difíciles de creer.

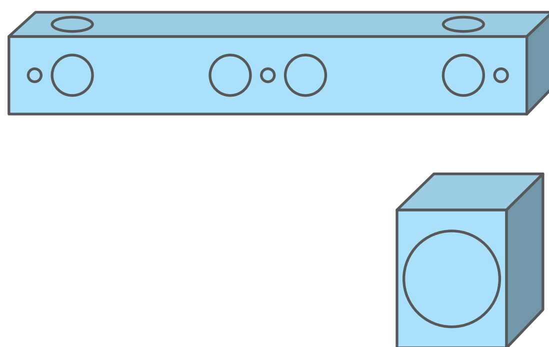


Fig. 5 Ejemplo de barra de sonido 3.1.2

Una solución bastante utilizada en sistemas con canal de sonido central, sean barras de sonido o baffles separados, es usar 2 woofers y un tweeter. Esta configuración se la conoce como DÁppolito, a partir del Ing. del mismo nombre. Busca que el centro acústico de los dos woofers y el tweeter sea uno solo, y esto mejora la inteligibilidad de los diálogos.

Sistemas 5.1

Son los conocidos sistema de home theater o teatro en casa. Canal frontal izquierdo, frontal central, frontal derecho, trasero izquierdo, trasero derecho y subwoofer. Es importante que la decodificación de la señal para obtener el deseado sonido envolvente se efectúe de forma adecuada, sobre todo en la actualidad con la variedad de formatos codificados de sonido que existen. Nunca está de más chequear este tema, conociendo que por ejemplo muchos contenidos on line no brindan la posibilidad por defecto. La idea es obligar al sistema a reproducir contenido de este tipo, conociendo de antemano que la fuente original puede proveerlo. Dolby Digital o DTS son sistemas conocidos con esta codificación. Por ejemplo, actualmente en Youtube existe la posibilidad de escuchar de esta manera, pero no todos los Smart TV o decodificadores lo realizan de forma apropiada.

Sistemas 5.1.2

Canal frontal izquierdo, frontal central, frontal derecho, trasero izquierdo, trasero derecho, techo izquierdo, techo derecho y subwoofer.

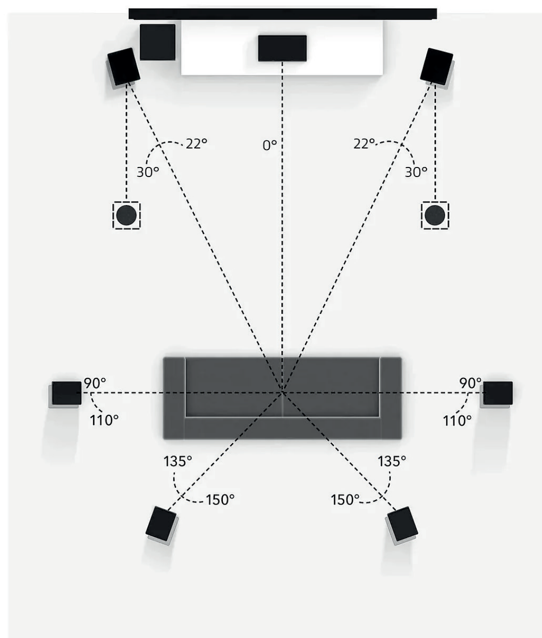


Fig. 6 Ejemplo de Sistema 5.1.2

Sistemas 5.2.2

Canal frontal izquierdo, frontal central, frontal derecho, trasero izquierdo, trasero derecho, techo izquierdo, techo derecho y 2 subwoofers. Últimamente existen diseños que incorporan dos subwoofers a los canales conocidos. Este diseño busca tener más flexibilidad en el posicionamiento de los subwoofers, para evitar ondas estacionarias siempre presentes en los ambientes domésticos. De hecho, en la actualidad, muchos equipos incluyen alguna forma de medir las bajas frecuencias en la propia instalación, para tener en cuenta las particularidades de los ambientes. Este tema es más importante de lo que inicialmente puede parecernos, y amerita por lo menos un artículo solamente dedicado a ello. Podríamos citar que al ir elevando la calidad del equipamiento, después de un cierto umbral, la interacción con el ambiente donde se reproducen los sonidos comienza a ser más relevante que los equipos en sí mismos, sea esto tanto para sistemas 2.0 como los de sonido envolvente.

Esperamos que el presente artículo aporte algo de "luz" en el interesante tema de los sistemas de sonido.